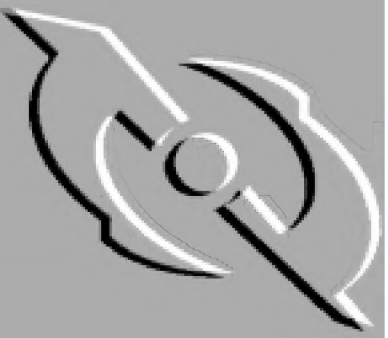

McAfee VirusScan for Windows 95 and Windows 98

User's Guide

Version 4.0.1

Network Associates UK
Minton Place, Victoria St.
Windsor, Berkshire
SL4 1 EG
UK

Network Associates Canada
139 Main Street, Suite 201
Unionville, Ontario
L3R 2G9
Canada

Network Associates Australia
Level 1, 500 Pacific Highway
St. Leonards
NSW 2065
Australia

COPYRIGHT

Copyright © 1998-1999 Network Associates, Inc. and its Affiliated Companies. All Rights Reserved. No part of this publication may be reproduced, transmitted, transcribed, stored in a retrieval system, or translated into any language in any form or by any means without the written permission of Network Associates, Inc.

LICENSE AGREEMENT

NOTICE TO ALL USERS: CAREFULLY READ THE FOLLOWING LEGAL AGREEMENT ("AGREEMENT"), WHICH SETS FORTH GENERAL LICENSE TERMS FOR NETWORK ASSOCIATES SOFTWARE. FOR THE SPECIFIC TERMS OF YOUR LICENSE, CONSULT THE README.1ST, LICENSE.TXT, OR OTHER LICENSE DOCUMENT THAT ACCOMPANIES YOUR SOFTWARE, EITHER AS A TEXT FILE OR AS PART OF THE SOFTWARE PACKAGING. IF YOU DO NOT AGREE TO ALL OF THE TERMS SET FORTH THEREIN, DO NOT INSTALL THE SOFTWARE. (IF APPLICABLE, YOU MAY RETURN THE PRODUCT TO THE PLACE OF PURCHASE FOR A FULL REFUND.)

1. **License Grant.** Subject to the payment of the applicable license fees and subject to the terms and conditions of this Agreement, Network Associates hereby grants to you a non-exclusive, non-transferable right to use one copy of the specified version of the Software and the accompanying documentation (the "Documentation"). You may install one copy of the Software on one computer, workstation, personal digital assistant, pager, "smart phone" or other electronic device for which the Software was designed (each, a "Client Device"). If the Software is licensed as a suite or is bundled with more than one specified Software product, this license applies to all such specified Software products, subject to any restrictions or usage terms specified individually for any of such Software products on the applicable product invoicing or packaging.

   a. **Use.** The Software is licensed as a single product; it may not be used on more than one Client Device or by more than one user at a time, except as set forth in this Section 1. The Software is "in use" on a computer when it is loaded into the temporary memory (i.e., random-access memory or RAM) or installed into the permanent memory (e.g., hard disk, CD-ROM, or other storage device) of that Client Device. This license authorizes you to make one copy of the Software solely for backup or archival purposes, provided that the copy you make contains all proprietary notices.

   b. **Server Use.** To the extent that the applicable product invoicing or packaging sets forth, you may install and use the Software on a Client Device or as a server ("Server") within a multi-user or networked environment ("Server Use") for either (i) connecting, directly or indirectly, to not more than the maximum number of specified Client Devices or "seats"; or (ii) deploying not more than the maximum number of agents (pollers) specified for deployment. If the applicable product invoicing or packaging does not specify a maximum number of Client Devices or pollers, this license gives you a single product use license subject to the provisions of subsection (a) above. A separate license is required for each Client Device or seat that can connect to the Software at any time, regardless of whether such licensed Client Devices or seats are connected to the Software concurrently, or are actually using the Software at any particular time.

Your use of software or hardware that reduces the number of Client Devices or seats that connect to and use the Software simultaneously (e.g., using "multiplexing" or "pooling" hardware or software) does not reduce the number of licenses you must have in total. Specifically, you must have that number of licenses that would equal the number of distinct inputs to the multiplexing or pooling software or hardware "front end." If the number of Client Devices or seats that can connect to the Software can exceed the number of licenses that you have obtained, then you must have a reasonable mechanism in place to ensure that your use of the Software does not exceed the use limits set forth in the product invoicing or packaging. This license authorizes you to make or download one copy of the Documentation for each Client Device or seat that is licensed, provided that each such copy contains all of the proprietary notices for the Documentation.

c. **Volume Use.** If the Software is licensed with volume use terms specified in the applicable product invoicing or packaging, you may make, use and install as many additional copies of the Software on the number of Client Devices as the volume use terms specify. This license authorizes you to make or download one copy of the Documentation for each such copy of the Software you may make according to the volume use terms, provided that each such copy contains all of the proprietary notices for the Documentation. You must have a reasonable mechanism in place to ensure that the number of Client Devices on which the Software is installed does not exceed the number of licenses you have obtained.

2. **Term.** This license is effective for the period of time specified in the product invoicing or packaging, or in the README.1ST, LICENSE.TXT, or other text file that accompanies the Software and purports to set forth the terms of your license agreement. Where the provisions of the Agreement set forth here conflict with the provisions of the product invoicing or packaging, the README.1ST document, the LICENSE.TXT document, the product invoice, package, or the other text document will constitute the terms of your license grant to use the Software. Either you or Network Associates may terminate your license earlier than the period specified in the appropriate document in accordance with the terms set forth therein. This Agreement and your license will terminate automatically if you fail to comply with any of the limitations or other requirements described. When this agreement terminates, you must destroy all copies of the Software and Documentation. You may terminate this Agreement at any point by destroying the Software and Documentation together with all copies of the Software and Documentation.

3. **Updates.** During the term of your license, you may download revisions, upgrades, or updates to the Software when Network Associates publishes them via its electronic bulletin board system, website or through other online services.

4. **Ownership Rights.** The Software and the Documentation are protected by United States copyright laws and international treaty provisions. Network Associates owns and retains all right, title and interest in and to the Software, including all copyrights, patents, trade secret rights, trademarks and other intellectual property rights therein. You acknowledge that your possession, installation, or use of the Software does not transfer to you any title to the intellectual property in the Software, and that you will not acquire any rights to the Software except as expressly set forth in this Agreement. You agree that any copies of the Software and Documentation will contain the same proprietary notices that appear on and in the Software and Documentation.

5. **Restrictions.** You may not rent, lease, loan or resell the Software, or permit third parties to benefit from the use or functionality of the Software via a timesharing, service bureau or other arrangement. You may not transfer any of the rights granted to you under this Agreement. You may not copy the Documentation accompanying the Software. You may not reverse engineer, decompile, or disassemble the Software, except to the extent that the foregoing restriction is expressly prohibited by applicable law. You may not modify, or create derivative works based upon the Software in whole or in part. You may not copy the Software except as expressly permitted in Section 1 above. You may not remove any proprietary notices or labels on the Software. All rights not expressly set forth hereunder are reserved by Network Associates. Network Associates reserves the right to periodically conduct audits upon advance written notice to verify compliance with the terms of this Agreement.

6. **Warranty and Disclaimer**

   a. **Limited Warranty.** Network Associates warrants that for thirty (30) days from the date of original purchase or distribution the media (for example, the diskettes) on which the Software is contained will be free from defects in materials and workmanship.

   b. **Customer Remedies.** Network Associates' and its suppliers' entire liability, and your exclusive remedy, shall be, at Network Associates' option, either (i) return of the purchase price paid for the license, if any, or (ii) replacement of the defective media on which the Software is contained with a copy on non-defective media. You must return the defective media to Network Associates at your expense with a copy of your receipt. This limited warranty is void if the defect has resulted from accident, abuse, or misapplication. Any replacement media will be warranted for the remainder of the original warranty period. Outside the United States, this remedy is not available to the extent that Network Associates is subject to restrictions under United States export control laws and regulations.

   Warranty Disclaimer. To the maximum extent permitted by applicable law, and except for the limited warranty set forth herein, THE SOFTWARE IS PROVIDED ON AN "AS IS" BASIS WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. WITHOUT LIMITING THE FOREGOING PROVISIONS, YOU ASSUME RESPONSIBILITY FOR SELECTING THE SOFTWARE TO ACHIEVE YOUR INTENDED RESULTS, AND FOR THE INSTALLATION OF, USE OF, AND RESULTS OBTAINED FROM THE SOFTWARE. WITHOUT LIMITING THE FOREGOING PROVISIONS, NETWORK ASSOCIATES MAKES NO WARRANTY THAT THE SOFTWARE WILL BE ERROR-FREE OR FREE FROM INTERRUPTIONS OR OTHER FAILURES, OR THAT THE SOFTWARE WILL MEET YOUR REQUIREMENTS. TO THE MAXIMUM EXTENT PERMITTED BY LAW, NETWORK ASSOCIATES DISCLAIMS ALL WARRANTIES, EITHER EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, AND NONINFRINGEMENT WITH RESPECT TO THE SOFTWARE AND THE ACCOMPANYING DOCUMENTATION. SOME STATES AND JURISDICTIONS DO NOT ALLOW LIMITATIONS ON IMPLIED WARRANTIES, SO THE ABOVE LIMITATIONS MIGHT NOT APPLY TO YOU. The foregoing provisions shall be enforceable to the maximum extent permitted by applicable law.

Your purchase of or payment for the Software may entitle you to additional warranty rights, which Network Associates will specify in the product invoicing or packaging you received with your purchase, or in the README.1ST , LICENSE.TXT or other text file that accompanies the Software and purports to set forth the terms of your license agreement. Where the provisions of this Agreement conflict with the provisions of the product invoice or packaging, the README.1ST, the LICENSE.TXT, or similar documents, the invoice, packaging, or text file will set forth the terms of your warranty rights for the Software.

7. **Limitation of Liability.** UNDER NO CIRCUMSTANCES AND UNDER NO LEGAL THEORY, WHETHER IN TORT, CONTRACT, OR OTHERWISE, SHALL NETWORK ASSOCIATES OR ITS SUPPLIERS BE LIABLE TO YOU OR TO ANY OTHER PERSON FOR ANY INDIRECT, SPECIAL, INCIDENTAL, OR CONSEQUENTIAL DAMAGES OF ANY CHARACTER INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF GOODWILL, WORK STOPPAGE, COMPUTER FAILURE OR MALFUNCTION, OR FOR ANY AND ALL OTHER DAMAGES OR LOSSES. IN NO EVENT WILL NETWORK ASSOCIATES BE LIABLE FOR ANY DAMAGES IN EXCESS OF THE LIST PRICE NETWORK ASSOCIATES CHARGES FOR A LICENSE TO THE SOFTWARE, EVEN IF NETWORK ASSOCIATES SHALL HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. THIS LIMITATION OF LIABILITY SHALL NOT APPLY TO LIABILITY FOR DEATH OR PERSONAL INJURY TO THE EXTENT THAT APPLICABLE LAW PROHIBITS SUCH LIMITATION. FURTHERMORE, SOME STATES AND JURISDICTIONS DO NOT ALLOW THE EXCLUSION OR LIMITATION OF INCIDENTAL OR CONSEQUENTIAL DAMAGES, SO THIS LIMITATION AND EXCLUSION MAY NOT APPLY TO YOU. The foregoing provisions shall be enforceable to the maximum extent permitted by applicable law.

8. **United States Government.** The Software and accompanying Documentation are deemed to be "commercial computer software" and "commercial computer software documentation," respectively, pursuant to DFAR Section 227.7202 and FAR Section 12.212, as applicable. Any use, modification, reproduction, release, performance, display or disclosure of the Software and accompanying Documentation by the United States Government shall be governed solely by the terms of this Agreement and shall be prohibited except to the extent expressly permitted by the terms of this Agreement.

9. **Export Controls.** Neither the Software nor the Documentation and underlying information or technology may be downloaded or otherwise exported or re-exported (i) into (or to a national or resident of) Cuba, Iran, Iraq, Libya, North Korea, Sudan, Syria or any other country to which the United States has embargoed goods; or (ii) to anyone on the United States Treasury Department's list of Specially Designated Nations or the United States Commerce Department's Table of Denial Orders. By downloading or using the Software, you are agreeing to the foregoing provisions and you are certifying that you are not located in, under the control of, or a national or resident of any such country or on any such list.

   IN ADDITION, YOU SHOULD BE AWARE THAT EXPORT OF THE SOFTWARE MAY BE SUBJECT TO COMPLIANCE WITH THE RULES AND REGULATIONS PROMULGATED FROM TIME TO TIME BY THE BUREAU OF EXPORT ADMINISTRATION, UNITED STATES DEPARTMENT OF COMMERCE, WHICH

RESTRICT THE EXPORT AND RE-EXPORT OF CERTAIN PRODUCTS AND TECHNICAL DATA. IF THE EXPORT OF THE SOFTWARE IS CONTROLLED UNDER SUCH RULES AND REGULATIONS, THEN THE SOFTWARE SHALL NOT BE EXPORTED OR RE-EXPORTED, DIRECTLY OR INDIRECTLY, (A) WITHOUT ALL EXPORT OR RE-EXPORT LICENSES AND UNITED STATES OR OTHER GOVERNMENTAL APPROVALS REQUIRED BY ANY APPLICABLE LAWS, OR (B) IN VIOLATION OF ANY APPLICABLE PROHIBITION AGAINST THE EXPORT OR RE-EXPORT OF ANY PART OF THE SOFTWARE. SOME COUNTRIES HAVE RESTRICTIONS ON THE USE OF ENCRYPTION WITHIN THEIR BORDERS, OR ON THE IMPORT OR EXPORT OF ENCRYPTION EVEN IF FOR ONLY TEMPORARY BUSINESS OR PERSONAL USE. YOU ACKNOWLEDGE THAT THE IMPLEMENTATION AND ENFORCEMENT OF THESE LAWS IS NOT ALWAYS CONSISTENT AS TO SPECIFIC COUNTRIES. ALTHOUGH THE FOLLOWING COUNTRIES ARE NOT AN EXHAUSTIVE LIST, THERE MAY EXIST RESTRICTIONS ON THE EXPORTATION OF ENCRYPTION TECHNOLOGY TO, OR IMPORTATION FROM: BELGIUM, CHINA (INCLUDING HONG KONG), FRANCE, INDIA, INDONESIA, ISRAEL, RUSSIA, SAUDI ARABIA, SINGAPORE, AND SOUTH KOREA. YOU ACKNOWLEDGE THAT IT IS YOUR RESPONSIBILITY TO COMPLY WITH ANY AND ALL GOVERNMENT EXPORT AND OTHER APPLICABLE LAWS, AND THAT NETWORK ASSOCIATES HAS NO FURTHER RESPONSIBILITY AFTER THE INITIAL SALE TO YOU WITHIN THE ORIGINAL COUNTRY OF SALE.

11. **High Risk Activities.** The Software is not fault-tolerant and is not designed or intended for use in hazardous environments requiring fail-safe performance, including without limitation, in the operation of nuclear facilities, aircraft navigation or communication systems, air traffic control, weapons systems, direct life-support machines, or any other application in which the failure of the Software could lead directly to death, personal injury, or severe physical or property damage (collectively, "High Risk Activities"). Network Associates expressly disclaims any express or implied warranty of fitness for High Risk Activities.

12. **Miscellaneous.** This Agreement is governed by the laws of the United States and the State of California, without reference to conflict of laws principles. The application of the United Nations Convention of Contracts for the International Sale of Goods is expressly excluded. The Agreement set forth here is advisory in nature and does not supersede the provisions of any Agreement set forth in the README.1ST, LICENSE.TXT, or other text file that accompanies the Software and purports to set forth the terms of your license agreement. Where the provisions of this Agreement conflict with the provisions of the README.1ST or the LICENSE.TXT document, the text document will constitute the terms of your license grant to use the Software. This Agreement may not be modified except by a written addendum issued by a duly authorized representative of Network Associates. No provision hereof shall be deemed waived unless such waiver shall be in writing and signed by Network Associates or a duly authorized representative of Network Associates. If any provision of this Agreement is held invalid, the remainder of this Agreement shall continue in full force and effect. The parties confirm that it is their wish that this Agreement has been written in the English language only.

13. **Network Associates Customer Contact.** If you have any questions concerning these terms and conditions, or if you would like to contact Network Associates for any other reason, please call (408) 988-3832, fax (408) 970-9727, write Network Associates, Inc. at 3965 Freedom Circle, Santa Clara, California 95054, or visit the Network Associates website at http://www.nai.com.

Table of Contents

Preface xiii

What happened? xiii

Why worry? xiii

Where do viruses come from? xiv

Virus prehistory xiv

Viruses and the PC revolution xv

On the frontier xviii

Java and ActiveX xviii

Where next? xix

How to protect yourself xx

How to contact Network Associates xxi

Customer service xxi

Technical support xxi

Network Associates training xxii

Comments and feedback xxii

Reporting new items for anti-virus data file updates xxiii

International contact information xxiv

Chapter 1. About McAfee VirusScan 27

What is VirusScan? 27

What comes with VirusScan? 28

Deciding when to scan for viruses 31

Recognizing when you don't have a virus 31

Chapter 2. Installing McAfee VirusScan 33

Before You Begin 33

System requirements 33

Installation Steps 34

Performing a "silent" installation 44

Validating Your Files 50

Testing Your Installation 52

Chapter 3. Removing Infections From Your System 53
If you suspect you have a virus... 53
Creating an emergency disk 55
Creating an Emergency Disk without the utility 59
Responding to viruses or malicious software 60
Understanding false detections 71

Chapter 4. Using VShield 73
What does VShield do? 73
Why use VShield? 73
Which browsers and e-mail clients does VShield support? 74
Using the VShield configuration wizard 75
Setting VShield properties 81
Using VShield's shortcut menu 132
Disabling or stopping VShield 132
Tracking VShield status information 136

Chapter 5. Using McAfee VirusScan 139
What is VirusScan? 139
Why run on-demand scan operations? 139
Starting VirusScan 140
Using VirusScan menus 141
Configuring VirusScan Classic 143
Configuring VirusScan Advanced 149
Starting VirusScan Advanced 149

Chapter 6. Scheduling Scan Tasks 165
What does VirusScan Scheduler do? 165
Why schedule scan operations? 165
Starting the VirusScan Scheduler 166
Using the Scheduler window 167
Working with default tasks 169
Creating new tasks 170
Enabling tasks 172
Checking task status 175

Configuring task options 176
Configuring VirusScan for scheduled scanning 176
Configuring AutoUpdate options 196
Configuring AutoUpgrade options 206
Configuring options for other programs 215

Chapter 7. Using Specialized Scanning Tools 217
Scanning Microsoft Exchange and Outlook mail 217
Configuring the E-Mail Scan program component 218
Scanning cc:Mail 229
Using ScreenScan 230

Appendix A. Using SecureCast to Update Your Software 235
Introducing SecureCast 235
Why would I need to update my data files? 236
Which data files does SecureCast deliver? 236
System requirements 236
SecureCast features 237
Free services 237
Home SecureCast Channel 237
Understanding SecureCast 237
Downloading automatically 238
Initiating a Download 239
Updating registered software 239
Registering evaluation software 246
Enterprise SecureCast Channel 250
Benefits 250
Setting up Enterprise SecureCast 251
Using Enterprise SecureCast 252
Troubleshooting Enterprise SecureCast 252
Unsubscribing from Enterprise SecureCast 253
Support Resources 254
SecureCast 254

BackWeb 254

Appendix B. Network Associates Support Services 255

PrimeSupport Options for Corporate Customers 255

PrimeSupport Basic 255

PrimeSupport Extended 256

PrimeSupport Anytime 256

Ordering PrimeSupport 258

Support Services for Retail Customers 258

Network Associates Consulting and Training 259

Professional Consulting Services 259

Total Education Services 260

Appendix C. Understanding the .VSC File Format 261

Saving VirusScan task settings 261

ScanOptions 262

DetectionOptions 262

ActionOptions 264

ReportOptions 265

ScanItems 266

SecurityOptions 267

ExcludedItems 268

Appendix D. Understanding the .VSH File Format 269

Saving VShield configuration options 269

System Scan module 270

E-Mail Scan module 277

Download Scan module 284

Internet Filter module 289

Security module 293

General Settings 293

Appendix E. Using VirusScan Command-Line Options 295

Running VirusScan Command line 295
Command line options 296

Index 305

Preface

What happened?

If you've ever lost important files stored on your hard disk, watched in dismay as your computer ground to a halt only to display a prankster's juvenile greeting on your monitor, or found yourself having to apologize for abusive e-mail messages you never sent, you know first-hand how computer viruses and other harmful programs can disrupt your productivity. If you haven't yet suffered from a virus "infection," count yourself lucky. But with more than 24,000 known viruses in circulation capable of attacking Windows- and DOS-based computer systems, it really is only a matter of time before you do.

The good news is that of those thousands of circulating viruses, only a small proportion have the means to do real damage to your data. In fact, the term "computer virus" identifies a broad array of programs that have only one feature in common: they "reproduce" themselves automatically by attaching themselves to host software or disk sectors on your computer, usually without your knowledge. Most viruses cause relatively trivial problems, ranging from the merely annoying to the downright insignificant. Often, the primary consequence of a virus infection is the cost you incur in time and effort to track down the source of the infection and eradicate all of its traces.

Why worry?

So why worry about virus infections, if most attacks do little harm? The problem is twofold. First, although relatively few viruses have destructive effects, that fact says nothing about how widespread the malicious viruses are. In many cases, viruses with the most debilitating effects are the hardest to detect—the virus programmer bent on causing harm will take extra steps to avoid discovery. Second, even "benign" viruses can interfere with the normal operation of your computer and can cause unpredictable behavior in other software. Some viruses contain bugs, poorly written code, or other problems severe enough to cause crashes when they run. Other times, legitimate software has problems running when a virus has, intentionally or otherwise, altered system parameters or other aspects of the computing environment. Tracking down the source of resulting system freezes or crashes drains time and money from more productive activities.

Beyond these problems lies a problem of perception: once infected, your computer can serve as a source of infection for other computers. If you regularly exchange data with colleagues or customers, you could unwittingly pass on a virus that could do more damage to your reputation or your dealings with others than it does to your computer.

The threat from viruses and other malicious software is real, and it is growing worse. Some estimates have placed the total worldwide cost in time and lost productivity for merely detecting and cleaning virus infections at $1 billion per year, a figure that doesn't include the costs of data loss and recovery in the wake of attacks that destroyed data.

Where do viruses come from?

As you or one of your colleagues recovers from a virus attack or hears about new forms of malicious software appearing in commonly used programs, you've probably asked yourself a number of questions about how we as computer users got to this point. Where do viruses and other malicious programs come from? Who writes them? Why do those who write them seek to interrupt workflows, destroy data, or cost people the time and money necessary to eradicate them? What can stop them?

Why did this happen to me?

It probably doesn't console you much to hear that the programmer who wrote the virus that erased your hard disk's file allocation table didn't target you or your computer specifically. Nor will it cheer you up to learn that the virus problem will probably always be with us. But knowing a bit about the history of computer viruses and how they work can help you better protect yourself against them.

Virus prehistory

Historians have identified a number of programs that incorporated features now associated with virus software. Canadian researcher and educator Robert M. Slade traces virus lineage back to special-purpose utilities used to reclaim unused file space and perform other useful tasks in the earliest networked computers. Slade reports that computer scientists at a Xerox Corporation research facility called programs like these "worms," a term coined after the scientists noticed "holes" in printouts from computer memory maps that looked as though worms had eaten them. The term survives to this day to describe programs that make copies of themselves, but without altering host software.

A strong academic tradition of computer prank playing most likely contributed to the shift away from utility programs and toward more malicious uses of the programming techniques found in worm software. Computer science students, often to test their programming abilities, would construct rogue worm programs and unleash them to "fight" against each other, competing to see whose program could "survive" while shutting down rivals. Those same students also found uses for worm programs in practical jokes they played on unsuspecting colleagues.

Some of these students soon discovered that they could use certain features of the host computer's operating system to give them unauthorized access to computer resources. Others took advantage of users who had relatively little computer knowledge to substitute their own programs—written for their own purposes—in place of common or innocuous utilities. These unsophisticated users would run what they thought was their usual software only to find their files erased, to have their account passwords stolen, or to suffer other unpleasant consequences. Such "Trojan horse" programs or "Trojans," so dubbed for their metaphorical resemblance to the ancient Greek gift to the city of Troy, remain a significant threat to computer users today.

Viruses and the PC revolution

What we now think of as true computer viruses first appeared, according to Robert Slade, soon after the first personal computers reached the mass market in the early 1980s. Other researchers date the advent of virus programs to 1986, with the appearance of the "Brain" virus. Whichever date has the better claim, the link between the virus threat and the personal computer is not coincidental.

The new mass distribution of computers meant that viruses could spread to many more hosts than before, when a comparatively few, closely guarded mainframe systems dominated the computing world from their bastions in large corporations and universities. Nor did the individual users who bought PCs have much use for the sophisticated security measures needed to protect sensitive data in those environments. As further catalyst, virus writers found it relatively easy to exploit some PC technologies to serve their own ends.

Boot-sector viruses

Early PCs, for example, "booted" or loaded their operating systems from floppy disks. The authors of the Brain virus discovered that they could substitute their own program for the executable code present on the boot sector of every floppy disk formatted with Microsoft's MS-DOS, whether or not it included system files. Users thereby loaded the virus into memory every time they started their computers with any formatted disk in their floppy drives. Once in memory, a virus can copy itself to boot sectors on other floppy or hard disks. Those who unintentionally loaded Brain from an infected floppy found themselves reading an ersatz "advertisement" for a computer consulting company in Pakistan.

With that advertisement, Brain pioneered another characteristic feature of modern viruses: the payload. The payload is the prank or malicious behavior that, if triggered, causes effects that range from annoying messages to data destruction. It's the virus characteristic that draws the most attention—many virus authors now write their viruses specifically to deliver their payloads to as many computers as possible.

For a time, sophisticated descendants of this first boot-sector virus represented the most serious virus threat to computer users. Variants of boot sector viruses also infect the Master Boot Record (MBR), which stores the partition information your computer needs to figure out where to find each of your hard disk partitions and the boot sector itself.

Realistically, nearly every step in the boot process, from reading the MBR to loading the operating system, is vulnerable to virus sabotage. Some of the most tenacious and destructive viruses still include the ability to infect your computer's boot sector or MBR among their repertoire of tricks. Among other advantages, loading at boot time can give a virus a chance to do its work before your anti-virus software has a chance to run. VirusScan anticipates this possibility by allowing you to create an emergency disk you can use to boot your computer and remove infections.

But boot sector and MBR viruses have a particular weakness: they must spread by means of floppy disks or other removable media, riding concealed in that first track of disk space. As fewer users exchange floppy disks and as software distribution has come to rely on other media, such as CD-ROMs, other virus types have recently eclipsed the boot sector threat. The popularity of large-capacity floppy disks like the Iomega Zip disk and similar disks from other vendors, however, could cause a resurgence.

File infector viruses

At about the same time as the authors of the Brain virus found vulnerabilities in the DOS boot sector, other virus writers found out how to use existing software to help replicate their creations. An early example of this type of virus showed up in computers at Lehigh University in Pennsylvania. The virus infected part of the DOS command interpreter COMMAND.COM, which it used to load itself into memory. Once there, it spread to other uninfected COMMAND.COM files each time a user entered any standard DOS command that involved disk access. This limited its spread to floppy disks that contained, usually, a full operating system.

Later viruses quickly overcame this limitation, sometimes with fairly clever programming. Virus writers might, for instance, have their virus add its code to the beginning of an executable file, so that when users start a program, the virus code executes immediately, then transfers control back to the legitimate software, which runs as though nothing unusual has happened. Once it activates, the virus "hooks" or "traps" requests that legitimate software makes to the operating system and substitutes its own responses. Particularly clever viruses can even subvert attempts to clear them from memory by trapping the CTRL+ALT+DEL keyboard sequence for a warm reboot, then faking a restart. Sometimes the only outward indication that anything on your system is amiss—before any payload detonates, that is—might be a small change in the file size of infected legitimate software.

Stealth, mutating, encrypted, and polymorphic viruses

Unobtrusive as they might be, changes in file size and other scant evidence of a virus infection usually gives most anti-virus software enough of a scent to locate and remove the offending code. One of the virus writer's principal challenges, therefore, is to find ways to hide his or her handiwork. The earliest disguises were a mixture of innovative programming and obvious giveaways. The Brain virus, for instance, redirected requests to see a disk's boot sector away from the actual location of the infected sector to the new location of the boot files, which the virus had moved. This "stealth" capability enabled this and other viruses to hide from conventional search techniques.

Because viruses needed to avoid continuously reinfecting host systems—doing so would quickly balloon an infected file's size to easily detectable proportions or would consume enough system resources to point to an obvious culprit—their authors also needed to tell them to leave certain files alone. They addressed this problem by having the virus write a code "signature" that would flag infected files with the software equivalent of a "do not disturb" sign. Although that kept the virus from giving itself away immediately, it opened the way for anti-virus software to use the code signatures themselves to find the virus.

In response, virus writers found ways to conceal the code signatures. Some viruses would "mutate" or write different code signatures with each new infection. Others encrypted most of the code signature or the virus itself, leaving only a couple of bytes to use as a key for decryption. The most sophisticated new viruses employed stealth, mutation and encryption to appear in an almost undetectable variety of new forms. Finding these "polymorphic" viruses required software engineers to develop very elaborate programming techniques for anti-virus software.

Macro viruses

By 1995 or so, the virus war had come to something of a standstill. New viruses appeared continuously, prompted in part by the availability of ready-made virus "kits" that enabled even some non-programmers to whip up a new virus in no time. But most existing anti-virus software easily kept pace with updates that detected and disposed of the new virus variants, which consisted primarily of minor tweaks to well-known templates.

But 1995 marked the emergence of the Concept virus, which added a new and surprising twist to virus history. Before Concept, most virus researchers thought of data files—the text, spreadsheet, or drawing documents created by the software you use—as immune to infection. Viruses, after all, are programs and, as such, needed to be able to run in the same way executable software did in order to do their damage. Data files, on the other hand, simply stored information that you entered when you worked with your software.

That distinction melted away when Microsoft began adding macro capabilities to Word and Excel, the flagship applications in its Office suite. Using the stripped-down version of its Visual BASIC language included with the suite, users could create document templates that would automatically format and add other features to documents created with Word and Excel. Virus writers seized the opportunity that this presented to conceal and spread viruses in documents that you, the user, created yourself.

The exploding popularity of the Internet and of e-mail software that allowed users to attach files to messages ensured that macro viruses would spread very quickly and very widely. Within a year, macro viruses became the most potent virus threat ever.

On the frontier

Even as viruses grow more sophisticated and continue to threaten the integrity of computer systems we all have come to depend upon, still other dangers have begun to emerge from an unexpected source: the World Wide Web. Once a repository of research papers and academic treatises, the web has transformed itself into perhaps the most versatile and adaptable medium ever invented for communication and commerce.

Because its potential seems so vast, the web has attracted the attention and the developmental energies of nearly every computer-related company in the industry. Convergences in the technologies that have resulted from this feverish pace of invention now give web page designers tools they can use to collect and display information in ways never previously available. Websites can now send and receive e-mail, formulate and execute queries to databases using advanced search engines, send and receive live audio and video, and distribute data and multimedia resources to a worldwide audience.

Much of the technology that makes these features possible consists of small, easily downloaded programs that interact with your browser software and, sometimes, with other software on your hard disk. This same avenue can serve as an entry point into your computer system for other—less benign—programs to use for their own purposes.

Java and ActiveX

These programs, whether beneficial or harmful, come in a variety of forms. Some are special-purpose miniature applications, or "applets," written in Java, a new programming language first developed by Sun Microsystems. Others are developed using ActiveX, a Microsoft technology that programmers can use for similar purposes.

Both Java and ActiveX make extensive use of prewritten software modules, or "objects," that programmers can write themselves or take from existing sources and fashion into the plug-ins, applets, device drivers and other software needed to power the web. Java objects are called "classes," while ActiveX objects are called "controls." The principle difference between them lies in how they run on the host system. Java applets run in a Java "virtual machine" designed to interpret Java programming and translate it into action on the host machine, while ActiveX controls run as native Windows software that links and passes data among other Windows programs.

The overwhelming majority of these objects are useful, even necessary, parts of any interactive website. But despite the best efforts of Sun and Microsoft engineers to design security measures into them, determined programmers can use Java and ActiveX tools to plant harmful objects on websites, where they can lurk until visitors unwittingly allow them access to vulnerable computer systems.

Unlike viruses, harmful Java and ActiveX objects usually don't seek to replicate themselves. The web provides them with plenty of opportunities to spread to target computer systems, while their small size and innocuous nature makes it easy for them to evade detection. In fact, unless you tell your web browser specifically to block them, Java and ActiveX objects download to your system automatically whenever you visit a website that hosts them.

Instead, harmful objects exist to deliver their equivalent of a virus payload. Programmers have written objects, for example, that can read data from your hard disk and send it back to the website you visited, that can "hijack" your e-mail account and send out offensive messages in your name, or that can watch data that passes between your computer and other computers.

Where next?

Malicious software has even begun intruding into areas once thought completely out of bounds. Users of the mIRC Internet Relay Chat client, for example, have reported encountering viruses constructed from the mIRC scripting language. The chat client sends script viruses as plain text, which would ordinarily preclude them from infecting systems, but older versions of the mIRC client software would interpret the instructions coded into the script and perform unwanted actions on the recipient's computer. The vendors moved quickly to disable this capability in updated versions of the software, but the mIRC incident illustrates the general rule that where a way exists to exploit a software security hole, someone will find it and use it.

Some virus writers do it for the thrill of it, some to gain notoriety in their own peer group. Still others do it to exact revenge against employers or others they believe have treated them badly. Whatever their motives, they continue to develop new ways to cause you trouble.

How to protect yourself

VirusScan's advanced protection already gives you an important bulwark against infection and damage to your data, but anti-virus software is only one part of the security measures you should take to protect yourself. Anti-virus software, moreover, is only as good as its latest update. Because as many as 200 to 300 viruses and variants appear each month, the data (.DAT) files that enable Network Associates software to detect and remove viruses can get quickly outdated. If you have not updated the files that originally came with your software, you could risk infection from newly emerging viruses. Because Network Associates has assembled the world's largest and most experienced anti-virus research staff within its McAfee Labs division, however, the updated files you need to combat new viruses appear as soon as—and often before—you need them.

Most other security measures are common sense—checking disks you receive from unknown or questionable sources, either with anti-virus software or some kind of verification utility, is always a good idea. Malicious programmers have gone so far as to mimic the programs you trust to guard your computer, pasting a familiar face on software with a less-than-friendly purpose. VirusScan includes the VALIDATE.EXE utility with its distributions to prevent this type of manipulation, but neither it nor any anti-virus software can detect when someone substitutes an as-yet unidentified Trojan horse or other malicious program for one of your favorite shareware or commercial utilities.

Web and Internet access poses its own risks. VirusScan gives you the ability to block dangerous web sites so that users can't inadvertently download malicious software from known hazards; it also catches hostile objects that get downloaded anyway. But having a top-notch firewall in place to protect your network and implementing other network security measures is a necessity when unscrupulous attackers can penetrate your network from nearly any point on the globe, whether to steal sensitive data or implant malicious code. You should also make sure that your network is not accessible to unauthorized users, and that your have an adequate training program in place to teach and enforce security standards. To learn about the origin, behavior and other characteristics of particular viruses, consult the Virus Information Library maintained on the Network Associates website.

Network Associates can provide you with other software in the Total Virus Defense (TVD) suite, the most comprehensive anti-virus solution available, and Total Network Security (TNS), the industry's most advanced network security suite. Network Associates backs them both with outstanding support, training and a worldwide network of research and development teams. Contact your Network Associates representative, or visit the Network Associates website, to find out how to enlist the power of Total Virus Defense on your side.

How to contact Network Associates

Customer service

To order products or obtain product information, contact the Network Associates Customer Care department at (408) 988-3832 or write to the following address:

Network Associates International
Gatwickstraat 25
1043 GL Amsterdam
The Netherlands

Technical support

Network Associates is famous for its dedication to customer satisfaction. We have continued this tradition by making our site on the World Wide Web a valuable resource for answers to technical support issues. We encourage you to make this your first stop for answers to frequently asked questions, for updates to Network Associates software, and for access to Network Associates news and virus information.

World Wide Web	http://support.nai.com

If you do not find what you need or do not have web access, try one of our automated services.

Automated Voice and Fax Response System	(408) 988-3034
Internet	support@nai.com
CompuServe	GO NAI
America Online	keyword MCAFEE

If the automated services do not have the answers you need, contact Network Associates at one of the following numbers Monday through Friday between 6:00 A.M. and 6:00 P.M. Pacific time.

For corporate-licensed customers:

Phone	(408) 988-3832
Fax	(408) 970-9727

For retail-licensed customers:

Phone	(972) 278-6100
Fax	(408) 970-9727

To provide the answers you need quickly and efficiently, the Network Associates technical support staff needs some information about your computer and your software. Please have this information ready before you call:

- Product name and version number
- Computer brand and model
- Any additional hardware or peripherals connected to your computer
- Operating system type and version numbers
- Network type and version, if applicable
- Contents of your AUTOEXEC.BAT, CONFIG.SYS, and system LOGIN script
- Specific steps to reproduce the problem

Network Associates training

For information about scheduling on-site training for any Network Associates product, call (800) 338-8754.

Comments and feedback

Network Associates appreciates your comments and reserves the right to use any information you supply in any way it believes appropriate without incurring any obligation whatsoever. Please address your comments about Network Associates anti-virus product documentation to: Network Associates, Inc., 15220 NW Greenbrier Parkway, Suite 100, Beaverton, OR 97006-5762, U.S.A. You can also send faxed comments to (503) 531-7655 or e-mail to tvd_documentation@nai.com.

Reporting new items for anti-virus data file updates

Network Associates anti-virus software offers you the best available detection and removal capabilities, including advanced heuristic scanning that can detect new and unnamed viruses as they emerge. Occasionally, however, an entirely new type of virus that is not a variation on an older type can appear on your system and escape detection. Because Network Associates researchers are committed to providing you with effective and up-to-date tools you can use to protect your system, please tell them about any new Java classes, ActiveX controls, dangerous websites, or viruses that your software does not now detect. Note that Network Associates reserves the right to use any information you supply as it deems appropriate, without incurring any obligations whatsoever. Send your suggestions to:

virus_research@nai.com	Use this address to report new virus strains, harmful ActiveX controls and Java classes, or dangerous Internet sites.

To report items to our European research office, use this e-mail address:

virus_research_europe@nai.com

To report items to our Asia-Pacific research office, or our office in Japan, use one of these e-mail addresses:

avert-jp@nai.com	Use this address to report harmful items to our office in Japan.
avert_apac@nai.com	Use this address to report harmful items to our Asia-Pacific office.

International contact information

To contact Network Associates outside the United States, use the addresses, phone numbers and fax numbers below.

Network Associates Australia

Level 1, 500 Pacific Highway
St. Leonards, NSW
Sydney, Australia 2065
Phone: 61-2-8425-4200
Fax: 61-2-9439-5166

Network Associates Austria

Pulvermuehlstrasse 17
Linz, Austria
Postal Code A-4040
Phone: 43-732-757-244
Fax: 43-732-757-244-20

Network Associates Belgium

Bessenveldtstraat 25a
Diegem
Belgium - 1831
Phone: 32-2-716-4070
Fax: 32-2-716-4770

Network Associates do Brasil

Rua Geraldo Flausino Gomez 78
Cj. - 51 Brooklin Novo - São Paulo
SP - 04575-060 - Brasil
Phone: (55 11) 5505 1009
Fax: (55 11) 5505 1006

Network Associates Canada

139 Main Street, Suite 201
Unionville, Ontario
Canada L3R 2G6
Phone: (905) 479-4189
Fax: (905) 479-4540

Network Associates People's Republic of China

New Century Office Tower, Room 1557
No. 6 Southern Road Capitol Gym
Beijing
People's Republic of China 100044
Phone: 8610-6849-2650
Fax: 8610-6849-2069

NA Network Associates Oy

Kielotie 14 B
01300 Vantaa
Finland
Phone: 358 9 836 2620
Fax: 358 9 836 26222

Network Associates France S.A.

50 Rue de Londres
75008 Paris
France
Phone: 33 1 44 908 737
Fax: 33 1 45 227 554

Network Associates Deutschland GmbH

Industriestrasse 1
D-82110 Germering
Germany
Phone: 49 8989 43 5600
Fax: 49 8989 43 5699

Network Associates Srl

Centro Direzionale Summit
Palazzo D/1
Via Brescia, 28
20063 - Cernusco sul Naviglio (MI)
Italy
Phone: 39 (0)2 9214 1555
Fax: 39 (0)2 9214 1644

Network Associates Latin America

150 South Pine Island Road, Suite 205
Plantation, Florida 33324
United States
Phone: (954) 452-1731
Fax: (954) 236-8031

Network Associates International B.V.

Gatwickstraat 25
1043 GL Amsterdam
The Netherlands
Phone: 31 20 586 6100
Fax: 31 20 586 6101

Network Associates Hong Kong

19/F, Matheson Centre
3 Matheson Street
Causeway Bay
Hong Kong
Phone: 852-2832-9525
Fax: 852-2832-9530

Network Associates Japan, Inc.

Toranomon 33 Mori Bldg.
3-8-21 Toranomon Minato-Ku
Tokyo 105-0001
Japan
Phone: 81 3 5408 0700
Fax: 81 3 5408 0781

Network Associates de Mexico

Andres Bello No. 10, 4 Piso
4th Floor
Col. Polanco
Mexico City, Mexico D.F. 11560
Phone: (525) 282-9180
Fax: (525) 282-9183

Network Associates Portugal

Rua Gen. Ferreira Martins, 10-6°C
1495 Algés
Portugal
Phone: 351 1 412 1077
Fax: 351 1 412 1488

Net Tools Network Associates South Africa

Bardev House, St. Andrews
Meadowbrook Lane
Epson Downs, P.O. Box 7062
Bryanston, Johannesburg
South Africa 2021
Phone: 27 11 706-1629
Fax: 27 11 706-1569

Network Associates South East Asia

7 Temasek Boulevard
The Penthouse
#44-01, Suntec Tower One
Singapore 038987
Phone: 65-430-6670
Fax: 65-430-6671

Network Associates Spain

Orense 4, 4th Floor
Edificio Trieste
28020 Madrid
Spain
Phone: 34 91 598 18 00
Fax: 34 91 556 14 01

Network Associates Sweden

Datavägen 3A
Box 596
S-175 26 Järfälla
Sweden
Phone: 46 (0) 8 580 100 00
Fax: 46 (0) 8 580 100 05

Network Associates AG

Baeulerwisenstrasse 3
8152 Glattbrugg
Switzerland
Phone: 0041 1 808 99 66
Fax: 0041 1 808 99 77

Network Associates International Ltd.

Minton Place, Victoria Street
Windsor, Berkshire
SL4 1EF
United Kingdom
Phone: 44 (0)1753 827 500
Fax: 44 (0)1753 827 520

About McAfee VirusScan 1

What is VirusScan?

VirusScan is the key desktop element in the Network Associates Total Virus Defense suite of security tools. It acts as a tireless online sentry, guarding your system against attacks from viruses and preventing harm from other malicious software. Its powerful set of scanning tools and other enhancements have kept it at the front rank of anti-virus software, but with this latest release, VirusScan adds McAfee WebScanX technology to its protective arsenal—an improvement that helps to keep you safe from threats to your system that have begun to emerge from the Internet.

Advanced web page designs, for example, can incorporate interactive elements composed of Java classes and ActiveX controls. At the same time, millions of users now exchange messages, files and other data via e-mail, often using "attachments" that consist of executable files, document templates and other data. But these convenient new technologies can also hide new dangers. Executable files infected with viruses can lurk on websites, often without the site owner's knowledge, or can spread via e-mail, whether solicited or not. Sophisticated programmers can design Java applets or ActiveX controls that circumvent the security features built into your browser software to read data stored on your computer's hard disk, forge e-mail messages to others in your name, or cause other types of harm.

In this environment, taking precautions to protect yourself from malicious software is no longer a luxury, but a necessity. Consider the extent to which you rely on the data on your computer and the time, trouble and money it would take to replace that data if it became corrupted or unusable because of a virus infection. Balance that possibility against the time and effort it takes to put a few common sense security measures in place, and you can quickly see the utility in protecting yourself against infection.

Even if your own data is relatively unimportant to you, neglecting to guard against viruses might mean that your computer could play unwitting host to a virus that could spread to computers that your co-workers and colleagues use. Checking your hard disk periodically with VirusScan significantly reduces your vulnerability to infection and keeps you from losing time, money and data unnecessarily.

VirusScan gives you the tools you need to keep your system intact and secure. Used properly as one part of a comprehensive security program that includes backups, meaningful password protection, training, and awareness, VirusScan can keep your computer safe from debilitating attacks and prevent the spread of malicious software throughout your network.

What comes with VirusScan?

VirusScan consists of several component sets that combine one or more related programs, each of which play a part in defending your computer against viruses and other malicious software. The component sets are:

- **Common Components.** This set consists of data files and other support files that many of the VirusScan component programs share. These files include VirusScan virus definition (.DAT) files, default configuration files, validation files, and other files.

- **Command-Line Scanner.** This set consists of a SCANPM.EXE, a powerful scanning agent for 32-bit environments, and BOOTSCAN.EXE, a smaller, specialized scanner. Both programs allow you to initiate targeted scan operations from the MS-DOS Prompt window or from protected MS-DOS mode. Ordinarily, you'll use VirusScan's graphical user interface (GUI) to perform most scanning operations, but if you have trouble starting Windows or if the VirusScan GUI components will not run in your environment, you can use the command-line scanners as a backup.

  SCANPM.EXE provides you with a full-featured scanner for 16- and 32-bit protected-mode DOS environments and includes support for extended memory and flexible memory allocations. To use the scanner, open an MS-DOS Prompt window or restart your computer in MS-DOS mode, then run SCANPM.EXE from the command line, together with the scan options you want. See Appendix E, "Using VirusScan Command-Line Options," for a list and description of available options.

  VirusScan uses BOOTSCAN.EXE on its Emergency Disk in order to provide you with a virus-free boot environment. When you run the Emergency Disk creation wizard, VirusScan copies BOOTSCAN.EXE, a specialized set of .DAT files, and boot files to a single floppy disk. With this disk, you can start your computer, then scan its memory and the Master Boot Record, the boot sector, and the system files on your hard disk.

  BOOTSCAN.EXE will not detect or clean macro viruses, but it will detect or clean other viruses that can jeopardize your VirusScan installation or infect files at system startup. Once you identify and respond to those viruses, you can safely run VirusScan to clean the rest of your system, provided you don't run any other programs in the meantime.

- **VirusScan.** This component gives you unmatched control over your scanning operations. You can initiate a scan operation at any time—a feature known as "on-demand" scanning—specify local and network disks as scan targets, choose how VirusScan will respond to any infections it finds, and see reports on its actions. You can start with VirusScan's basic configuration mode, then move to its advanced mode for maximum flexibility. See "Using McAfee VirusScan" on page 139 for details.

- **VShield.** This component gives you continuous anti-virus protection from viruses borne on floppy disks, brought in from your network, or loaded into memory. VShield starts when you start your computer, and stays in memory until you shut down. A flexible set of property pages allows you to tell VShield which parts of your system to scan, when to scan them, which parts to leave alone, and how to respond to any infected files it finds. In addition, VShield can alert you when it finds a virus, and can generate reports that summarize each of its actions.

  This latest VShield version includes technology that guards against hostile Java applets and ActiveX controls. With this new capability, VShield can automatically scan e-mail messages and attachments that you receive from the Internet via Lotus cc:Mail, Microsoft Mail or other mail clients that comply with Microsoft's Messaging Application Programming Interface (MAPI). It can also filter out hostile Java classes and ActiveX controls by comparing those that it encounters with a database of classes and controls known to cause harm. When it detects a match, VShield can alert you, or it can automatically deny harmful objects access to your system. VShield can also keep your computer from connecting to dangerous Internet sites. Simply designate the sites your browser software should not visit, and VShield automatically prevents access. Secure password protection for your configuration options prevents others from making unauthorized changes. The same convenient dialog box controls configuration options for all VShield modules. See "Using VShield" on page 73 for details.

- **cc:Mail Scan.** This component includes technology optimized for scanning Lotus cc:Mail mailboxes that do not use the MAPI standard. Install and use this component if your workgroup or network uses cc:Mail v7.x or earlier. See "Choosing Detection options" on page 97 for details.

- **MAPI Scanner**. This component allows you to scan, at your initiative, the Inbox or other mailboxes for MAPI-compliant e-mail client applications. Use it to supplement the continuous background scanning VShield provides for MAPI clients such as Microsoft Exchange and Microsoft Outlook. See "Scanning Microsoft Exchange and Outlook mail" on page 217 for details.

- **VirusScan Scheduler.** This component allows you to create tasks for VirusScan to perform. A "task" can include anything from running a scan operation on a set of disks at a specific time or interval, to setting up VShield to run with particular options. The Scheduler comes with a preset list of tasks that ensures a minimal level of protection for your system—you can, for example, immediately scan and clean your C: drive or all disks on your computer, and enable or disable VShield. See "Scheduling Scan Tasks" on page 165 for details.

- **McAfee ScreenScan**. This optional component scans your computer as your screen saver runs during idle periods. See "Using ScreenScan" on page 194 for details.

- **Documentation.** VirusScan documentation includes:
  - A printed *Getting Started Guide*, which introduces the product, provides installation instructions, outlines how to respond if you suspect your computer has a virus, and provides a brief product overview. The *Getting Started Guide* comes only with the VirusScan copies distributed on CD-ROM discs—you cannot download it from Network Associates website or from other electronic services.
  - This user's guide saved on the VirusScan CD-ROM or installed on your hard disk in Adobe Acrobat .PDF format. The VirusScan *User's Guide* describes in detail how to use VirusScan and includes other information useful as background or as advanced configuration options. Acrobat .PDF files are flexible online documents that contain hyperlinks, outlines and other aids for easy navigation and information retrieval.

    For best results when opening and printing the *User's Guide*, Network Associates recommends using Acrobat Reader 3.0 —Reader version 3.0.1 has difficulty correctly printing graphics included in the .PDF file.
  - An online help file. This file gives you quick access to hints and tips about how to use VirusScan. To open the help file from within VirusScan or from within VirusScan Scheduler, choose **Help Topics** from the **Help** menu.

    VirusScan also includes context-sensitive online help. Right-click buttons, lists or other elements within dialog boxes to see brief, descriptive help topics. Click **Help** buttons where you see them to open the main help file to a relevant topic.
  - A README.1ST or LICENSE.TXT file. This file outlines the terms of your license to use VirusScan. Read it carefully—by installing VirusScan you agree to its terms.
  - A WHATSNEW.TXT file. This file contains last-minute additions or changes to the documentation, lists any known behavior or other issues with the product release, and often describes new product features incorporated into incremental product updates. You'll find the WHATSNEW.TXT file at the root level of your VirusScan CD-ROM disc or in the VirusScan program folder—you can open and print it from Windows Notepad, or from nearly any word-processing software.

Deciding when to scan for viruses

Maintaining a secure computing environment means scanning for viruses regularly. Depending on the degree to which you swap floppy disks with other users, share files over your local area network, or interact with other computers via the Internet, scanning "regularly" could mean scanning as little as once a month, or as often as several times a day. Other good habits to cultivate include scanning right before you back up your data, scanning before you install new or upgraded software, particularly software you download from other computers, and scanning when you start or shut down your computer each day. Use VShield to scan your computer's memory and maintain a constant level of vigilance between scanning operations. Under most circumstances this should protect your system's integrity.

If you connect to the Internet frequently or download files often, you might want to supplement regular scans with scans based on certain events. VirusScan includes a default set of scanning tasks to help you monitor your system at likely points of virus entry, such as

- whenever you insert a floppy disk into your computer's floppy drive
- whenever you start an application or open a file
- whenever you connect to or map a network drive to your system

Even the most diligent scanning can miss new viruses, however, if your scanning software is not up to date. Your VirusScan purchase entitles you to free virus updates for the life of your product, so you can update frequently to keep current. If you install the Network Associates SecureCast client software, VirusScan will even tell you when you should update your data files and offer to download them for you. To learn how to update your software, see Appendix A, "Using SecureCast to Update Your Software" and "Configuring AutoUpdate options" on page 196.

Recognizing when you don't have a virus

Personal computers have evolved, in their short lifespan, into highly complex machines that run ever more complicated software. Even the most farsighted of the early PC advocates could never have imagined the tasks for which workers, scientists and others have harnessed the modern PC's speed, flexibility and power. But that power comes with a price: hardware and software conflicts abound, applications and operating systems crash, and hundreds of other problems can crop up in unlikely places. In some cases, these failures can resemble the sorts of effects that you see when you have a virus infection with a destructive payload. Other computer failures seem to defy explanation or diagnosis, so frustrated users blame virus infections, perhaps as a last resort.

Because viruses do leave traces, however, you can usually eliminate a virus infection as a possible cause for computer failure relatively quickly and easily. Running a full VirusScan system scan will uncover all of the known virus variants that can infect your computer, and quite a few of those that have no known name or defined behavior. Although that doesn't give you much help when your problem really results from an interrupt conflict, it does allow you to eliminate one possible cause. With that knowledge, you can then go on to troubleshoot your system with a full-featured system diagnosis utility such as McAfee Nuts & Bolts.

More serious is the confusion that results from virus-like programs, virus hoaxes, and real security breaches. Anti-virus software simply cannot detect or respond to such destructive agents as Trojan horse programs that have never appeared previously, security breaches that enable hackers to prevent network access and crash systems, or the perception that a virus exists where none in fact does.

The best way to determine whether your computer failure resulted from a virus attack is to run a complete scan operation, then pay attention to the results. If VirusScan does not report a virus infection, the chances that your problem results from one are slight—look to other causes for your difficulties. Furthermore, in the very rare event that VirusScan does miss a macro virus or another virus type that has in fact infected your system, the chances are relatively small that serious failures will follow in its wake. You can, however, rely on Network Associates researchers to identify, isolate, and update VirusScan immediately to detect and, if possible, remove the virus when you next encounter it. To learn how you can help the virus researchers help you, see "Reporting new items for anti-virus data file updates" on page xxiii.

Installing McAfee VirusScan 2

Before You Begin

Network Associates distributes McAfee VirusScan in two ways: as an archived file that you can download from the Network Associates website or from other electronic services; and on CD-ROM disc. Once you have downloaded a VirusScan archive or placed your VirusScan installation disc in your CD-ROM drive, the installation steps you follow after that are the same for each type of distribution. Review the system requirements shown below to verify that VirusScan will run on your system, then follow the installation steps on page 34.

NOTE: Some VirusScan component sets come only with the CD-ROM version of the product. Consult your sales representative for details.

System requirements

VirusScan will install and run on any IBM PC or PC-compatible computer equipped with:

- A processor equivalent to an Intel 80386, or later. Network Associates recommends at least an Intel Pentium-class or compatible processor.
- A CD-ROM drive. If you downloaded your copy of VirusScan, this is an optional item.
- At least 15MB of free hard disk space for a full installation.
- At least 8MB of free random-access memory (RAM).
- Either Microsoft Windows 95 or Windows 98.

Other recommendations

To take full advantage of VirusScan's automatic update features, you should have an Internet connection, either through your local-area network, or via a high-speed modem and an Internet service provider.

NOTE: Network Associates does *not* provide Internet connections. Contact a local service provider to learn about rates and terms of service, or see your system administrator to learn about connecting to the Internet through your office network.

Installation Steps

Note which type of VirusScan distribution you have, then follow the corresponding steps to prepare your files for installation.

- **If you downloaded your copy of VirusScan** from the Network Associates website, from a server on your local network, or from another electronic service, make a new, temporary folder on your hard disk, then use WinZip, PKZIP, or a similar utility to extract the VirusScan installation files to that temporary folder. You can download the necessary utilities from most online services.

  > **IMPORTANT:** If you suspect that your computer has a virus infection, download the VirusScan installation files onto a computer that is ***not*** infected. Install your copy on this computer, then use the McAfee Emergency Disk utility during setup to make a disk you can use to boot your infected computer and remove the virus. See "If you suspect you have a virus..." on page 53 for more information.

- **If your copy of VirusScan came on a CD-ROM disc**, insert that disc into your computer's CD-ROM drive.

If you inserted a CD-ROM disc, you should see a VirusScan welcome image similar to that shown in Figure 2-1 appear automatically.

Figure 2-1. McAfee VirusScan welcome image

To install VirusScan immediately, click **Install**, then skip to Step 3 on page 36 to continue with Setup.

If the welcome image does not appear, or if you are installing VirusScan from files you downloaded, start with Step 1.

Follow these steps:

1. Choose **Run** from the **Start** menu in the Windows taskbar.

   The Run dialog box will appear (Figure 2-2).

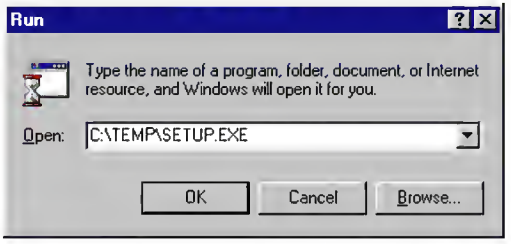

Figure 2-2. Run dialog box

2. Type `<X>:\SETUP.EXE` in the text box provided, then click **OK**.

   Here, `<X>` represents the drive letter for your CD-ROM drive or the path to the folder that contains your extracted VirusScan files. To search for the correct files on your hard disk or CD-ROM disc, click **Browse**.

   NOTE: If your VirusScan copy came on a VirusScan Security Suite or a Total Virus Defense CD-ROM disc, you must also specify which folder contains VirusScan for Windows 95 and Windows 98. See the CONTENTS.TXT file included with either CD-ROM disc for details.

   Setup will start and display its welcome panel (Figure 2-3).

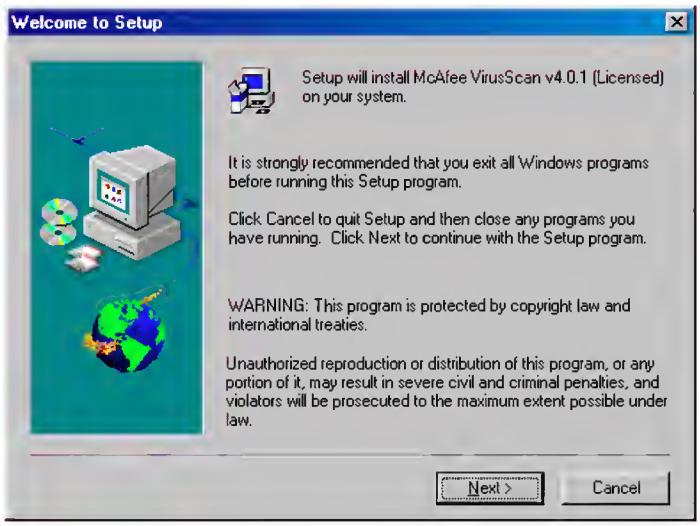
Welcome to Setup
Setup will install McAfee VirusScan v4.0.1 (Licensed) on your system.
It is strongly recommended that you exit all Windows programs before running this Setup program.
Click Cancel to quit Setup and then close any programs you have running. Click Next to continue with the Setup program.
WARNING: This program is protected by copyright law and international treaties.
Unauthorized reproduction or distribution of this program, or any portion of it, may result in severe civil and criminal penalties, and violators will be prosecuted to the maximum extent possible under law.
Next >
Cancel

Figure 2-3. Welcome to Setup wizard panel

3. Click **Next>** to continue.

   The next wizard panel displays the VirusScan end-user license agreement. Read this agreement carefully—if you install VirusScan, you agree to abide by the terms of the license.

4. If you do not agree to the license terms, click **No**. Setup will quit immediately. Otherwise, click **Yes** to continue.

   If you install this version of VirusScan over an existing version of VirusScan, Setup will detect the existing version and offer to remove it from your computer (Figure 2-4).

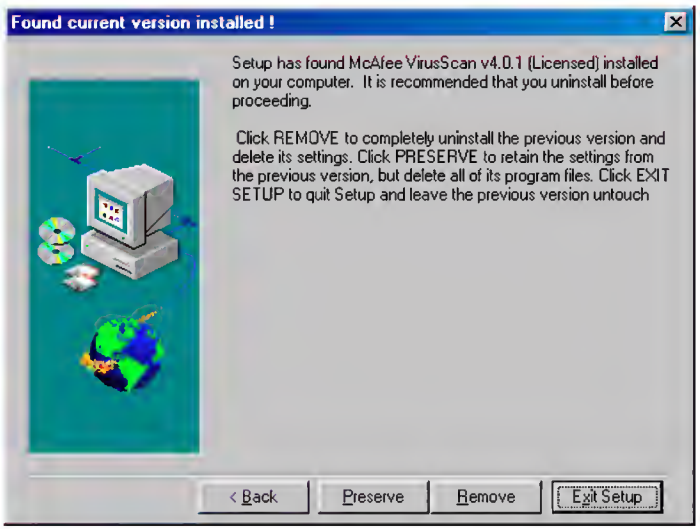
Found current version installed !
Setup has found McAfee VirusScan v4.0.1 (Licensed) installed on your computer. It is recommended that you uninstall before proceeding.
Click REMOVE to completely uninstall the previous version and delete its settings. Click PRESERVE to retain the settings from the previous version, but delete all of its program files. Click EXIT SETUP to quit Setup and leave the previous version untouch
< Back
Preserve
Remove
Exit Setup

Figure 2-4. Found Current Version Installed panel

5. To continue, you can

   - Click **Preserve** to retain the settings you chose for the existing VirusScan installation. Setup will retain the settings files, but will remove the rest of the VirusScan program files.

     NOTE: Setup will preserve settings only for VirusScan v4.0.1 and later. If will make every attempt to preserve settings from VirusScan v3.x, but will not attempt to preserve settings from VirusScan v2.x, or WebScanX v3.1.6 or earlier.

   - Click **Remove** to delete the existing VirusScan version and all of its settings from your computer. When it has finished removing the existing VirusScan version, Setup will display the panel shown in Figure 2-5 on page 38. You can then continue with Step 6.

   - Click **Exit Setup** to stop the installation altogether. Setup will prompt you to confirm that you want to quit. Click **Exit Setup** again to quit, or click **Resume** to continue with the installation.

   If you continue, Setup will remove your existing VirusScan version, making sure to preserve your earlier settings if you chose that option. When it finishes removing the earlier VirusScan version, it will display the Setup Type panel (Figure 2-5).

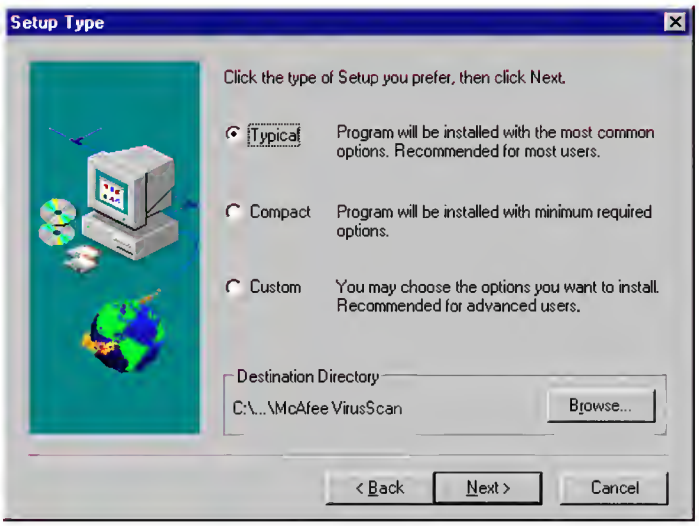
Setup Type
Click the type of Setup you prefer, then click Next.
Typical
Program will be installed with the most common options. Recommended for most users.
Compact
Program will be installed with minimum required options.
Custom
You may choose the options you want to install. Recommended for advanced users.
Destination Directory
C:\...\McAfee VirusScan
Browse...
< Back
Next >
Cancel

Figure 2-5. Setup Type panel

6. Select the VirusScan component sets that you want to install. You can choose from these options:

   - **Typical.** Select this option to install the VirusScan command-line scanner; the VirusScan on-demand scanner; the VShield on-access scanner; the MAPI client scanner; the VirusScan Scheduler, and common files that all program components use. Network Associates recommends this installation for most users.
   - **Compact.** Select this option to install the VirusScan command-line scanners, the VShield on-access scanner, and the VirusScan on-demand scanner. Network Associates recommends this option if you have minimal free disk space or other system constraints.
   - **Custom.** Select this option to choose which VirusScan components you want to install. By default, the Custom option installs the same components as the Typical installation, but you can also choose to install cc:Mail Scan, a plug-in option that enables VShield to look for viruses in your Lotus cc:Mail Inbox (See "Choosing Detection options" on page 97 for details), and ScreenScan, a scanning utility that examines your system for viruses whenever your screen saver activates.

7. Click **Browse** to locate the folder you want to use for the installation. By default, Setup installs VirusScan in this path:

   C:\Program Files\Network Associates\McAfee VirusScan

8. When you have chosen the component set that you want to install and have specified a destination, click **Next>** to continue.

   - **If you chose a Typical or a Compact component set**, Setup will show you a wizard panel that confirms your choice of components and the destination directory you specified. By default, Setup will look for existing viruses in your hard disk's partition and boot sectors, and in your computer's memory, before it installs VirusScan. Setup also adds a **Scan** command to the shortcut menus that appear when you right-click objects on your desktop or in Windows Explorer.

     If the options shown reflect your choices, click **Next>**. Otherwise, click **<Back** to change them. **Skip to** Step 9 on page 40.

   - **If you chose a Custom component set**, Setup shows you a wizard panel that lists the components available for installation (Figure 2-6). Select the components you want installed and clear the checkboxes next to those you don't want.

     As you select each component, a description appears near the bottom of the panel. When you have finished your selections, click **Next>**.

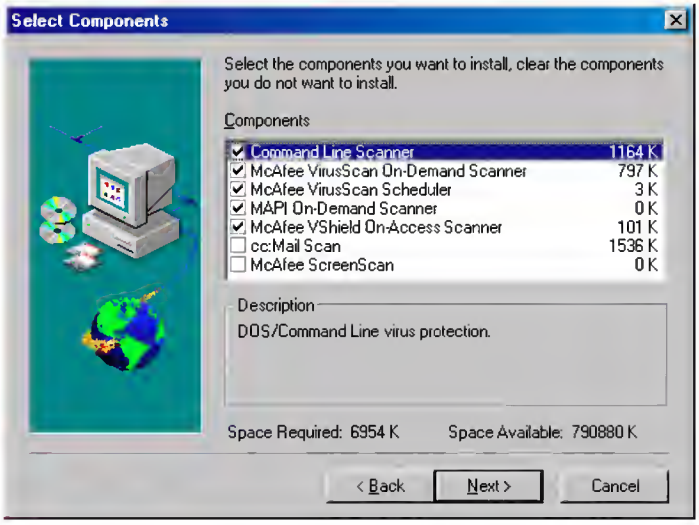
Select Components
Select the components you want to install, clear the components you do not want to install.
Components
Command Line Scanner 1164 K
McAfee VirusScan On-Demand Scanner 797 K
McAfee VirusScan Scheduler 3 K
MAPI On-Demand Scanner 0 K
McAfee VShield On-Access Scanner 101 K
cc:Mail Scan 1536 K
McAfee ScreenScan 0 K
Description
DOS/Command Line virus protection.
Space Required: 6954 K
Space Available: 790880 K
< Back
Next >
Cancel

Figure 2-6. Select Components panel

By default, Setup will have VirusScan look for existing viruses in your hard disk's partition and boot sectors, and in your computer's memory, before it completes installation. Setup will also add a Scan command to the shortcut menus that appear when you right-click an object on your desktop or in Windows Explorer. Click **Next>** at the bottom of each of the next two panels to continue.

If you do not want Setup to take these actions, clear each checkbox as it appears in each panel, then click **Next>** to continue.

Setup will next start VirusScan briefly to examine your hard disk and memory for viruses before it continues.

9. If VirusScan reports a clean system, click **OK** to continue. If VirusScan detects a virus infection, quit Setup immediately. See "If you suspect you have a virus..." on page 53 to learn what to do next.

10. Setup will begin copying VirusScan files to your computer. As it nears the end of the copy process, Setup will ask you whether you want to create an Emergency Disk (Figure 2-7).

Emergency Disk Wizard
Welcome to the McAfee Emergency Disk Creation Wizard.
This wizard will allow you to create a diskette that you can boot your system from in the event an unknown virus infects system files on your hard disk.
Click "Next" to continue or "Cancel" to quit.
Emergency Disk Wizard
< Back
Next >
Cancel

Figure 2-7. Emergency Disk Wizard panel

11. To skip this step, click **Cancel**, then move to Step 16—you can create an Emergency Disk after installation. To create an Emergency Disk now, click **Next>**.

NOTE: Network Associates strongly recommends that you create an Emergency Disk during installation, but after VirusScan has scanned your system for viruses. If VirusScan detects a virus on your system, do *not* create an Emergency Disk on the infected computer.

12. The next wizard panel appears (see Figure 2-8 on page 41). Here, you have two choices:

    - If you have a *virus-free, formatted* floppy disk that contains only DOS or Windows system files, insert it into your floppy drive. Next, select the **Don't format** checkbox, then click **Next>** to continue.

      This tells the Emergency Disk wizard to copy only the VirusScan Command Line component and its support files to the floppy disk. Skip to Step 13 on page 42 to continue.

Emergency Disk Wizard
Insert a blank high density diskette in drive A:.
Select "Next" to optionally format* the diskette and to copy the files to the diskette.
*Select "Don't format" if you wish to use a disk that is already bootable.
Don't format
Emergency Disk Wizard
< Back
Next >
Cancel

Figure 2-8. Second Emergency Disk Wizard panel

    - If you do *not* have a virus-free floppy disk formatted with DOS or Windows system files, you must create one in order to use the Emergency Disk to start your computer. Follow these substeps:

      a. Insert an *unformatted* floppy disk into your floppy drive.

      b. Verify that the **Don't format** checkbox is clear.

      c. Click **Next>**.

         The Windows disk format dialog box appears (Figure 2-9).

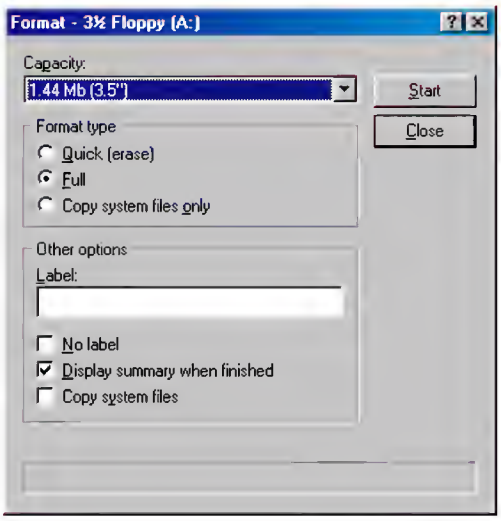

Figure 2-9. Windows format dialog box

d. Verify that the **Full** checkbox in the **Format type** area and the **Copy system files** checkbox in the **Other Options** area are both selected. Next, click **Start**.

   Windows will format your floppy disk and copy the system files necessary to start your computer.

e. Click **Close** when Windows has finished formatting your disk, then click **Close** again to return to the Emergency Disk panel.

13. Click **Next>** to continue. Setup will scan your newly formatted disk for viruses (Figure 2-10).

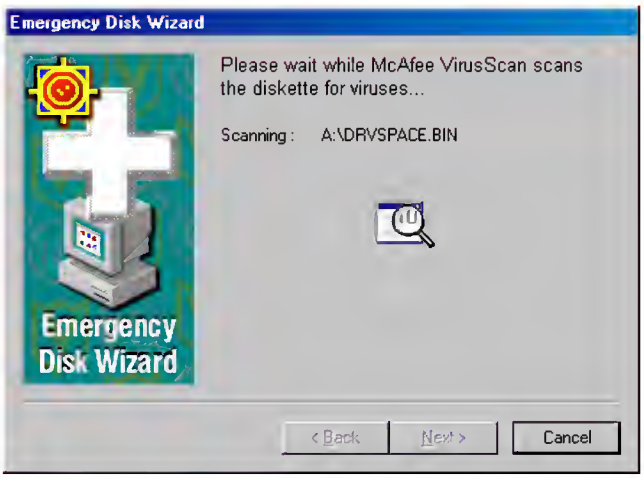
Emergency Disk Wizard
Please wait while McAfee VirusScan scans the diskette for viruses...
Scanning : A:\DRVSPACE.BIN
Emergency Disk Wizard
< Back
Next >
Cancel

Figure 2-10. Scanning Emergency Disk for viruses

If VirusScan does not detect any viruses during its scan operation, Setup will immediately copy BOOTSCAN.EXE and its support files to the floppy disk you created. If VirusScan *does* detect a virus, quit Setup immediately. See "If you suspect you have a virus..." on page 53 to learn what to do next.

14. When the wizard finishes copying the Emergency Disk files, it displays the final wizard panel (Figure 2-11).

Emergency Disk Wizard
An Emergency Disk has been created.
Label it -"McAfee Emergency Boot Disk".
Write protect it. To write protect the disk, open the write-protect notch in the upper corner of the disk.
To test your Emergency Disk, restart your computer with the disk in the A: drive. When you get to the A: prompt, type C: and press the ENTER key to access your hard drive. If you can access your hard drive in this test your Emergency Disk is functioning properly.
Store the disk in a safe place.
Emergency Disk Wizard
< Back
Finish
Cancel

Figure 2-11. Final Emergency Disk wizard panel

15. Click **Finish** to return to Setup. Next, remove the new Emergency Disk from your floppy drive, label it, lock it, and store it in a safe place.

NOTE: A locked floppy disk shows two holes near the edge of the disk opposite the metal shutter. If you don't see two holes, look for a plastic sliding tab at one of the disk corners, then slide the tab until it locks in an open position.

Setup will finish copying the VirusScan installation files to your hard disk, then it will list the names of the system files it changed. Setup lists AUTOEXEC.BAT because it adds a line to that file that tells VirusScan to run scan operation each time you start your computer. Setup also backs up your original AUTOEXEC.BAT file and renames it with a different extension in case you need to restore it.

16. Note the file name Setup uses to rename AUTOEXEC.BAT for future reference, then click **Next>** to continue.

17. Setup requires you to restart your computer in order to complete your VirusScan installation. This also ensures that the VShield component begins scanning for viruses immediately. If you have other work you must do, select **No, I will restart my computer later**, then click **Finish**. Otherwise, select **Yes, I want to restart my computer now**, then click **Finish** to reboot your system.

IMPORTANT: Network Associates strongly suggests that you reboot immediately in order to activate VShield's anti-virus protection. If you downloaded your VirusScan copy and want to validate it, do so *before* you reboot. See "Validating Your Files" to learn how to perform this check.

Performing a "silent" installation

If you manage a network and want to deploy VirusScan as your standard anti-virus security application, you can use the program's "silent" installation feature to set up VirusScan on each network node with little or no interaction from end users. During a silent installation, Setup does not display any of its usual wizard panels or windows, or offer the end user any configuration options. Instead, you preset these choices and run Setup in the background on each target workstation. If you wish, you can even install VirusScan on any unattended workstations or without the end user's knowledge, provided you have all the necessary administrative privileges.

A silent installation consists of two major steps. First, you must install the same VirusScan components on your administrative computer or server that you want Setup to install on each target workstation. A special Setup mode records the choices you make during installation and preserves them in a configuration file called SETUP.ISS. Next, you must use a different Setup mode to install an identical VirusScan configuration on each target system. Setup will use the SETUP.ISS file you create in the first step to guide each subsequent installation you perform.

Recording your preferences

To record your installation preferences, follow these steps:

1. Look for an existing SETUP.ISS file inside the \WINDOWS folder on your administrative computer or server. If you find a file with that name in the WINDOWS folder, rename it or delete it.

   As you record your installation preferences, Setup will save them into a new SETUP.ISS file in the same location.

2. Choose **Run** from the **Start** menu in the Windows taskbar.

   The Run dialog box will appear (Figure 2-12).

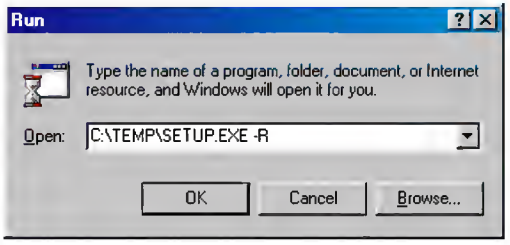

Figure 2-12. Run dialog box

3. Type `<X>:\SETUP.EXE -R` in the text box provided, then click **OK**.

   Here, `<X>` represents the drive letter for your CD-ROM drive or the path to the folder that contains your extracted VirusScan files. The `-R` tells Setup to run in its "record" mode.

> **NOTE:** If your VirusScan copy came on a VirusScan Security Suite or a Total Virus Defense CD-ROM disc, you must also specify which folder contains VirusScan for Windows 95 and Windows 98. See the CONTENTS.TXT file included with either product suite for details.

To search for SETUP.EXE on your hard disk or CD-ROM disc, click **Browse**. Be sure to add `-R` to the run statement if you use this option.

4. Follow the installation steps outlined on pages 37 to 44 to choose the components and the settings you want each of the target workstations to have.

Setup notes the choices you make at each step and records them as entries in SETUP.ISS.

IMPORTANT: Take particular care during this initial installation to respond to any questions that appear in the wizard panels and to follow the installation steps in the sequence presented, or the silent installation you run later will abort. You may not backtrack during the installation to change your settings.

To specify different options, you will need to begin the installation again in order for Setup to record your choices correctly. If you plan to install VirusScan on unattended workstations, be sure to specify options that do not require user interaction—don't ask Setup to create an Emergency Disk during installation, for example.

The installation will also abort if VirusScan detects a virus on your computer or server.

5. Once you've completed the installation, click **Finish** to quit Setup.

Editing the SETUP.ISS file to specify an installation directory

If you want Setup to install VirusScan in a particular directory, you will need to edit the SETUP.ISS file you created when you installed VirusScan on your administrative computer or server. To make network administration easier, for example, you might want to install all of your VirusScan copies in the same directory on each network node.

SETUP.ISS is simply a specially formatted text file similar to configuration files such as WIN.INI or SYSTEM.INI. You can open it in any text editor and change any of its entries to suit your needs.

NOTE: Network Associates recommends that you make only limited changes to the SETUP.ISS file. If you want complete control over the installation process, or if you want to specify the configuration options for each copy of VirusScan in advance, you can use ISeamless, a powerful Network Associates scripting tool designed for this purpose. Contact Network Associates Technical support for details.

SETUP.ISS specifies an installation directory as a value for the variable **szDir,** which you'll find listed beneath the header **[SdSetupType-0]**. By default, this entry reads:

```
[SdSetupType-0]
szDir=C:\Program Files\Network Associates\McAfee VirusScan\
Result=403
```

To specify a different installation directory, replace the path shown with the path you want. The installation directory you specify here will override the default installation directory on each target system.

IMPORTANT: Setup creates a unique SETUP.ISS file for each Network Associates product on each platform. You must use the file that corresponds to the operating system running on the target workstation. You may not, for example, use a SETUP.ISS file created during a VirusScan for Windows 95 installation to control a VirusScan for Windows NT installation.

6. Save the file in text format, then quit your text editor.

IMPORTANT: Network Associates recommends that you use the SETUP.ISS file you created to perform a test installation on a single workstation before you use it to deploy VirusScan across your network.

Running a silent installation

Once you have a SETUP.ISS file that lists all of the components and settings you want each workstation on your network to have, you can replicate these settings exactly for every VirusScan copy you install. See "Recording your preferences" on page 45 to learn how to create the SETUP.ISS file.

You can run a silent installation in a variety of ways, and with different levels of interaction with network users. You can, for example, create a script for your users that runs a silent VirusScan installation as soon as they connect to an authentication server, with no further interaction beyond that needed to log in. You can also ask your users to run the installation from a designated server. Still other options include deploying VirusScan through a network management application such as Zero Administration Client (ZAC) from Network Associates, System Management Server (SMS) from Microsoft, or similar packages.

Whichever method you choose, you must first prepare the VirusScan package for installation, then run Setup in its silent mode.

Follow these steps:

1. Copy the VirusScan installation files from the VirusScan CD-ROM disc or the folder on your administrative computer in which your store them to a VirusScan directory on a central server. Your users or your network management application will install VirusScan from this server.

2. Locate the SETUP.ISS file stored in the VirusScan directory on the central server. Rename or delete this file.

3. Copy the SETUP.ISS file you created when you ran the recorded installation on your administrative computer to the VirusScan directory on the central server. You'll find the file you need to copy in the WINDOWS directory on your administrative computer. See "Recording your preferences" on page 45 to learn how to record your installation.

   Once you finish this step, your users or your network management application can run Setup in its silent mode to replicate the installation you recorded.

To run Setup in silent mode, include the line `<X>:\SETUP.EXE -S` in any login script you write or any instructions to your users that describe how to run Setup. In this line, `<X>` represents the path to the folder on the server that contains the VirusScan installation files and the SETUP.ISS file you created. The `-S` tells Setup to run in silent mode. By default, Setup restarts the workstation when it has finished installing files.

If you do not want Setup to reboot each target workstation, you must edit the SETUP.ISS file you created during your recorded installation. Here, you would change the value in the **BootOption** entry beneath the heading **[sdFinishReboot - 0]** from its current value to zero (0). This tells Setup not to force the target workstation to reboot.

As a further step toward enforcing a consistent anti-virus security policy across your network, you can also copy a configuration file with the options you want your users to have into the installation directory on each workstation. You can also use password protection to prevent unauthorized changes to the configuration settings you chose. To learn how to save your settings in a configuration file, see "Using VirusScan menus" on page 141. To learn how to protect your settings with a password, see "Enabling password protection" on page 163.

NOTE: To preset your configuration options so that VirusScan installs with them already in place, use the Network Associates ISeamless scripting utility. This utility gives you complete control over installation and configuration options. Contact your sales representative or Network Associates technical support for details.

Validating Your Files

Downloading or copying files from any outside source places your computer at risk of virus infection—even if the risk is small. Downloading anti-virus software is no exception. Network Associates uses strict and extensive security measures to ensure that the products you purchase and download from its website and its other electronic services are safe, reliable, and free from virus infections. But anti-virus software tends to attract the attention of virus- and Trojan-horse writers, some of whom find it amusing to post infected copies of commercial software, or use the same file names to camouflage their own work.

You can protect yourself from this possibility, or from the possibility that the files you downloaded have become corrupted, by ensuring that you

- Download your files only from the Network Associates website; and
- Validate the files you download.

Network Associates includes a copy of VALIDATE.EXE, its validation software, with each VirusScan package.

To validate your files, follow these steps:

1. Install VirusScan as described in "Installation Steps" on pages 34 to 44.
2. Click **Start** in the Windows taskbar, point to **Programs**, then choose **MS-DOS Prompt**.
3. In the window that appears, change your command-line prompt to point to the directory that contains the VirusScan files you installed. If you chose the default installation options, you'll find the files in this path:

   C:\Program Files\Network Associates\McAfee VirusScan

   To get to this directory, type `cd progra~1\networ~1\mcafee~1` at the command-line prompt, then press ENTER. If you installed VirusScan in a different directory, type the correct path to that directory.
4. Run VALIDATE.EXE. To do so, type `validate *.*` at the command-line prompt.

   VALIDATE.EXE scans all of the files stored in your VirusScan program directory, then generates a file list that includes the file name, its size in bytes, its creation date and time, and two validation codes in separate columns.

To use VALIDATE.EXE to examine individual files, simply follow `validate` with the name of the file you want to verify at the prompt, or use the DOS wildcards `?` and `*` to specify a range of files.

NOTE: Network Associates recommends that you redirect the output from VALIDATE.EXE to your printer so that you can review it easily. If you have set your printer to capture output from MS-DOS programs, simply type `validate *.* >prn` at the command-line prompt. To learn how to set your printer to print from MS-DOS programs, consult your Windows documentation.

To ensure that you have exactly the same files as did the engineers who packaged your copy of VirusScan, you need to compare the validation codes against the packing list supplied with the program. The packing list is a text file that contains the validation codes that Network Associates engineers generated from independent cyclical redundancy check (CRC) processes when they packaged VirusScan for delivery. This method provides a high degree of security and prevents tampering.

5. To display the packing list, type `type packing.lst` at the command-line prompt, then press ENTER.

NOTE: Network Associates again recommends that you redirect the output from PACKING.LST to your printer. To do so, type `type packing.lst >prn` at the command-line prompt.

6. Compare the output from VALIDATE.EXE to that from PACKING.LST. The sizes, creation dates and times, and validation codes for each file name should match exactly. If they do not, delete the file immediately—do *not* open the file or examine it with any other utility; doing so can risk virus infection.

IMPORTANT: Checking your VirusScan installation with VALIDATE.EXE does not *guarantee* that your copy is free from defects, copying errors, virus infections or tampering, but the program's security features make it extremely unlikely that anyone has tampered with files that have correct validation codes. See the files LICENSE.TXT or README.1ST included with your copy of VirusScan to learn the license terms that cover your use of the program.

Testing Your Installation

Once you install it, VirusScan is ready to scan your system for infected files. You can test whether it has installed correctly and verify that it can properly scan for viruses by implementing a test developed by the European Institute of Computer Anti-virus Research (EICAR), a coalition of anti-virus vendors, as a method for their customers to test any anti-virus software installation.

To test your installation, follow these steps:

1. Open a standard Windows text editor, such as Notepad, then type:

```
X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-
TEST-FILE!$H+H*
```

> **NOTE:** The line shown above should appear as *one line* in your text editor window. If you are reading this manual on your computer, you can copy the line directly from the Acrobat file to Notepad.

2. Save the file with the name EICAR.COM. The file size will be 69 or 70 bytes.
3. Start VirusScan and allow it to scan the directory that contains EICAR.COM. When VirusScan examines this file, it will report finding the EICAR-STANDARD-AV-TEST-FILE virus.

> **IMPORTANT:** This file is *not a virus*—it cannot spread or infect other files, or otherwise harm your system. Delete the file when you have finished testing your installation to avoid alarming other users.

Removing Infections From Your System 3

If you suspect you have a virus...

First of all, don't panic! Although far from harmless, *most* viruses that infect your machine will not destroy data, play pranks, or render your computer unusable. Even the comparatively rare viruses that do carry a destructive payload usually produce their nasty effects in response to a trigger event. In most cases, unless you actually see evidence of a payload that has activated, you will have time to deal with the infection properly. The very presence of these small snippets of unwanted computer code can, however, interfere with your computer's normal operation, consume system resources and have other undesirable effects, so you should take them seriously and be sure to remove them when you encounter them.

A second idea to keep in mind is that odd computer behavior, unexplained system crashes, or other unpredictable events might have causes other than virus infections. If you believe you have a virus on your computer because of occurrences such as these, scanning for viruses might not produce the results you expect, but it will help eliminate one potential cause of your computer problems.

The safest course of action you can take is to install VirusScan and perform an immediate and thorough system scan.

As it installs itself, VirusScan will examine your computer's memory and your hard disk's boot sectors to verify that it can safely copy its files to your hard disk without risking their infection. If VirusScan reports during setup that your system appears virus-free, continue with the installation, then perform a full system scan as soon as you restart your computer—file-infector viruses that don't load into your computer's memory or hide in your hard disk's boot blocks might still be lurking somewhere on your system. See Chapter 2, "Installing McAfee VirusScan," to learn about virus scanning during setup. See Chapter 5, "Using McAfee VirusScan," to learn how to perform a full system scan.

If VirusScan detects a virus during Setup, you'll need to remove it from your system before you install the program. To learn how to do so, follow the steps that begin on page 54.

IMPORTANT: To ensure maximum security, you should follow these same steps if VirusScan detects a virus in your computer's memory later, after you have it installed.

If VirusScan found an infection during installation, follow these steps carefully:

1. Quit Setup immediately, then shut down your computer.

   Be sure to turn the power to your system off completely. Do *not* press CTRL+ALT+DEL or your computer's reset button to restart your system—some viruses can remain intact during this type of "warm" reboot.

2. If your copy of VirusScan came with an Emergency Disk, insert it into your floppy drive.

   ☐ **NOTE:** If your VirusScan copy did not come with a McAfee Emergency Disk, or if you have misplaced your Emergency Disk, you must create a new disk on an *uninfected* computer. Locate a computer that you know is virus-free, then follow the steps outlined in "Creating an emergency disk" on page 55.

3. Start your computer again.

   The Emergency Disk will boot your computer and immediately start BOOTSCAN.EXE, a special-purpose command-line scanner. The program will ask you whether you turned the power to your computer off before you started it with the Emergency Disk. If you did, press Y on your keyboard, then continue with Step 4. If you did not, press N, then turn your computer completely off and begin again.

   Once you start it, BootScan will report its progress as it scans your system, and will try to remove virus code from any infected files it finds. After it completes its scan operation, it will show you its final results: how many files it scanned; how many infected files it found; whether it found a virus in memory or in the boot blocks on your hard disk; and other information.

4. When BootScan finishes examining your system, you can either:

   - **Return to working with your computer.** If BootScan did not find a virus, or if it cleaned any infected files it did find, remove the Emergency Disk from your floppy drive, then restart your computer normally. If you had planned to install VirusScan on your computer but stopped when Setup found an infection, you can now continue with your installation.

   - **Try to clean or delete infected files yourself.** If BootScan found a virus that it could not remove, it will identify the infected files and tell you that it could not clean them, or that it does not have a current remover for the infecting virus.

As your next step, you can:

- **Locate and delete the infected file or files.** You will need to restore any files that you delete from backup files. Be sure to check your backup files for infections also.
- **Try to remove the infection yourself.** Network Associates supplies information and suggestions in its Virus Information Library that can help you remove a virus from an infected file. To see this information, start your preferred web browser application, then enter the following web address:

  http://www.nai.com/vinfo/<document number>.asp

  In the address listed, <document number> represents a technical document in the Virus Information Library. Replace <document number> with one of these numbers:

  0013 0319 0322 0323 0327 1145

  NOTE: Document numbers might change. See the online Virus Information Library table of contents for current information.

Creating an emergency disk

If you misplace your copy of the Emergency Disk that comes with VirusScan, or if you downloaded your VirusScan copy from one of the Network Associates electronic services, you will need to create an Emergency Disk.

WARNING: If VirusScan detected a virus as it tried to install itself on your computer, you must install VirusScan on an *uninfected* computer, then create your Emergency Disk on that system. After that, you can start the infected system with the Emergency Disk, remove the infecting virus, then install VirusScan on that system. Be sure to remove the VirusScan copy from the first system unless you have a license that allows you to install multiple VirusScan copies.

To create an Emergency Disk with the VirusScan Emergency Disk creation wizard, follow these steps:

1. Insert a blank, *unformatted* 1.44MB disk into your floppy drive.
2. Click **Start** in the Windows taskbar, point to **Programs**, then to **McAfee VirusScan**. Next, choose **Create Emergency Disk**.

The first Emergency Disk wizard panel will appear (Figure 3-1).

Emergency Disk Wizard
Welcome to the McAfee Emergency Disk Creation Wizard.
This wizard will allow you to create a diskette that you can boot your system from in the event an unknown virus infects system files on your hard disk.
Click "Next" to continue or "Cancel" to quit.
Emergency Disk Wizard
< Back
Next >
Cancel

Figure 3-1. Emergency Disk Wizard panel

3. Click **Next>** to display the next wizard panel (Figure 3-2). Here, you have two choices:

   - If you have a *virus-free, formatted* floppy disk that contains only DOS or Windows system files, insert it into your floppy drive. Next, select the **Don't format** checkbox, then click **Next>** to continue.

     This tells the Emergency Disk wizard to copy only the VirusScan Command Line component and its support files to the floppy disk. Skip to Step 5 on page 58 to continue.

Emergency Disk Wizard
Insert a blank high density diskette in drive A:. Select "Next" to optionally format* the diskette and to copy the files to the diskette.
*Select "Don't format" if you wish to use a disk that is already bootable.
Don't format
Emergency Disk Wizard
< Back
Next >
Cancel

Figure 3-2. Second Emergency Disk Wizard panel

- If you do *not* have a virus-free floppy disk formatted with DOS or Windows system files, you must create one in order to use the Emergency Disk to start your computer.

  Follow these substeps:

  a. Insert an *unformatted* floppy disk into your floppy drive.

  b. Verify that the **Don't format** checkbox is clear.

  c. Click **Next>**.

     The Windows disk format dialog box appears (Figure 3-3).

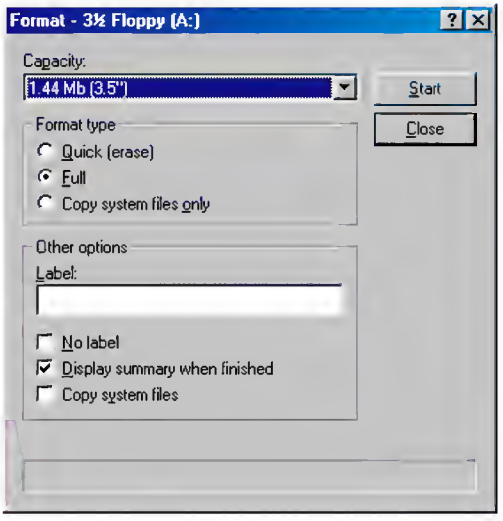

Figure 3-3. Windows format dialog box

  d. Verify that the **Full** checkbox in the **Format type** area and the **Copy system files** checkbox in the **Other Options** area are both selected. Next, click **Start**.

     Windows will format your floppy disk and copy the system files necessary to start your computer.

  e. Click **Close** when Windows has finished formatting your disk, then click **Close** again to return to the Emergency Disk wizard panel.

4. Click **Next>** to continue. This tells the Emergency Disk wizard to copy the VirusScan Command Line component and its support files to the bootable floppy disk you just created.

5. When the wizard finishes creating the Emergency Disk, click **Finish** to return to Setup. Label your new Emergency Disk, lock it, and store it in a safe place.

> **NOTE:** A locked floppy disk shows two holes near the edge of the disk opposite the metal shutter. If you don't see two holes, look for a plastic sliding tab at one of the disk corners, then slide the tab until it locks in an open position. Because no software can save to a locked disk, viruses cannot infect files stored on one.

Creating an Emergency Disk without the utility

If you cannot use the Emergency Disk creation utility because you have not yet installed VirusScan, or because VirusScan detected a virus during installation, you can create a clean Emergency Disk without the utility. Follow these steps:

WARNING: If VirusScan detected a virus as it tried to install itself on your computer, create your Emergency Disk on an *uninfected* computer.

1. Open an MS-DOS Prompt window or reboot your computer into DOS mode. To learn how to do so, consult your Windows documentation.
2. Insert a blank, *unformatted* 1.44MB disk into your floppy drive.
3. Type this command at the MS-DOS prompt:

   ```
   format <drive>: /s/u/v
   ```

   Substitute the drive letter for your floppy drive in place of `<drive>` in the command shown. Next, press **ENTER**. This tells your system to format the floppy disk you inserted, to overwrite any existing information on it, to copy DOS system files to it, and to have DOS prompt you to enter a volume label for it.
4. When DOS prompts you for a volume label, enter a name up to 11 characters long that distinguishes this disk from others.
5. If you have VirusScan installed on your computer and in its default program directory, change to the correct directory by typing this command at the MS-DOS prompt:

   ```
   cd\progra~1\networ~1\mcafee~1
   ```

   If you do not have VirusScan installed, change to the directory that contains the VirusScan files you extracted, or to the VirusScan directory on your CD-ROM drive.
6. Type the commands listed below at the MS-DOS prompt to copy the correct files to the Emergency Disk. Substitute the drive letter for your floppy drive in place of `<drive>` in the commands shown:

   ```
   copy bootscan.exe <drive>:

   copy scan.dat <drive>:

   copy names.dat <drive>:

   copy clean.dat <drive>:

   copy license.dat <drive>:

   copy messages.dat <drive>:

   copy edwiz16.exe <drive>:
   ```

7. Copy to the Emergency Disk any other DOS utilities you need to start your computer, debug your system software, manage any extended or expanded memory you have, or perform other tasks at startup. If you use a disk compression utility, be sure to copy the drivers you need to uncompress your files.

8. When you have finished copying files to the Emergency Disk, label it, lock it, and store it in a safe place.

> **NOTE:** A locked floppy disk shows two holes near the edge of the disk opposite the metal shutter. If you don't see two holes, look for a plastic sliding tab at one of the disk corners, then slide the tab until it locks in an open position. Because no software can save to a locked disk, viruses cannot infect files stored on one.

Responding to viruses or malicious software

Because VirusScan consists of several component programs, any one of which could be active at one time, your possible responses to a virus infection or to other malicious software will depend upon which program detected the harmful object, how you have that program configured to respond, and other circumstances. The following sections give an overview of the default responses available with each program component. To learn about other possible responses, see the chapter that discusses each component in detail.

Responding when VShield detects malicious software

VShield consists of four related modules that provide you with continuous background scanning protection against viruses, harmful Java and ActiveX objects, and dangerous websites. A fifth module controls security settings for the other four. You can configure and activate each module separately, or use them together to provide maximum protection. See Chapter 4, "Using VShield," to learn about each module's configuration options. Because each module detects different objects or scans different virus entry points, each has a different set of default responses.

System Scan module

By default, this module looks for viruses each time you run, copy, create, or rename any file on your system, or whenever you read from a floppy disk. Because it does so, System Scan can serve as a backup in case any of the other VShield modules does not detect a virus that you download with, for example, an FTP client application. In its initial configuration, when the module finds a virus during any of these operations, it will prevent you from opening, saving or copying the infected file and will ask you what you want to do about the virus (see Figure 3-4 on page 61).

The response options you see in this dialog box come from default choices or choices you make in the System Scan module's Action page. See "Choosing Action options" on page 87 to learn how to choose which options appear here.

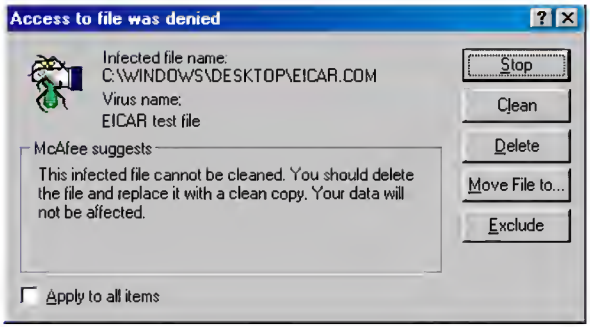

Figure 3-4. Initial System Scan response options

If you've selected the **Continue access** checkbox in the module's Action page, you'll see instead a full-screen warning that offers you response options (Figure 3-5).

Figure 3-5. System Scan response options

To take one of the listed actions, click a button in the dialog box, or type the letter highlighted in yellow when you see the full-screen warning. If you want the same response to apply to all infected files that VShield finds during this scan operation, select the **Apply to all items** checkbox in the dialog box. Your choices are:

- **Clean the file.** Click **Clean** in the dialog box, or type `C` when you see the full-screen warning, to tell VShield to try to remove the virus code from the infected file. If VShield succeeds, it will restore the file to its original state.

If VShield cannot clean the file—either because it has no remover or because the virus has damaged the file beyond repair—it will note this result in its log file, but will take no other action. In most cases, you should delete such files and restore them from backups.

- **Delete the file.** Click **Delete** in the dialog box, or type D when you see the full-screen warning, to tell VShield to delete the infected file immediately. By default, VShield notes the name of the infected file in its log file so that you have a record of which files it flagged as infected. You can then restore deleted files from backup copies.
- **Move the file to a different location.** Click **Move File to** in the dialog box. This opens a browse window you can use to locate your quarantine folder or another folder you want to use to isolate infected files. Once you select a folder, VShield moves the infected file to it immediately.
- **Continue working.** Type O when you see the full-screen warning to tell VShield to let you continue working with the file and not take any other action. Normally, you would use this option to bypass files that you know do not have viruses. If you have its reporting option enabled, VShield will note each incident in its log file.
- **Stop the scan operation.** Click **Stop** in the dialog box, or type S when you see the full-screen warning, to tell VShield to deny you any access to the file but not to take any other action. Denying access to the file prevents you from opening, saving, copying or renaming it. To continue, you must click **OK**. If you have its reporting option enabled, VShield will note each incident in its log file.
- **Exclude the file from scan operations.** Click **Exclude** in the dialog box, or type E when you see the full-screen warning, to tell VShield to exclude this file from future scan operations. Normally, you would use this option to bypass files that you know do not have viruses.

E-mail Scan module

This module looks for viruses in e-mail messages you receive via corporate e-mail systems such as cc:Mail and Microsoft Exchange. In its initial configuration, the module will prompt you to choose a response from among three options whenever it detects a virus (Figure 3-6). A fourth option provides you with additional information.

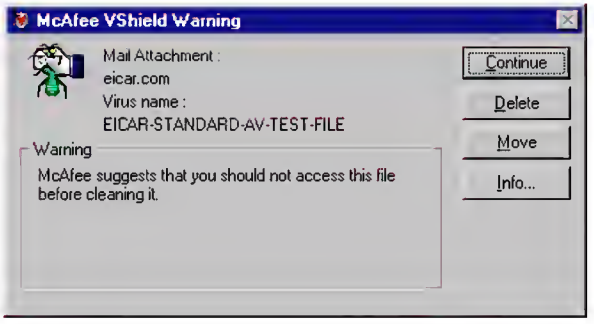

Figure 3-6. E-mail Scan module response options

Click the button that corresponds to the response you want. Your choices are:

- **Continue.** Click this to tell VShield to take no action and to resume scanning. VShield will continue until it finds another virus on your system or until it finishes the scan operation. Normally, you would use this option to bypass files that you know do not have viruses, or if you plan to leave your computer unattended as you download e-mail. VShield will note each incident in its log file.
- **Delete.** Click this to tell VShield to delete the infected file attachment from the e-mail message you received. By default, VShield notes the name of the attachment in its log file.
- **Move.** Click this to tell VShield to create a quarantine directory where it found the virus, then move the infected file to it. If you use Microsoft Exchange, Microsoft Outlook or other MAPI mail clients, for example, the quarantine directory will appear as a folder called INFECTED in your mailbox on the mail server. If you use a POP-3 or similar mail client, the quarantine folder will appear at the root level of your hard disk as soon as you download an infected file.
- **Info.** Click this to connect to the Network Associates Virus Information Library. This choice does not take any action against the virus VShield detected. See "Viewing File and Virus Information" on page 70 for details.

When you choose your action, VShield will implement it and add a notice to the top of the e-mail message that contained the infected attachment. The notice gives the file name of the infected attachment, identifies the name of the infecting virus, and describes the action VShield took in response.

Download Scan module

This module looks for viruses in e-mail messages and other files you receive over the Internet via a web browser or such e-mail client programs as Eudora Light, Netscape Mail, Outlook Express, and others. It will *not* detect files you download with FTP client applications, terminal applications, or through similar channels. In its initial configuration, the module will prompt you to choose a response from among three options whenever it detects a virus (Figure 3-7). A fourth option provides you with additional information.

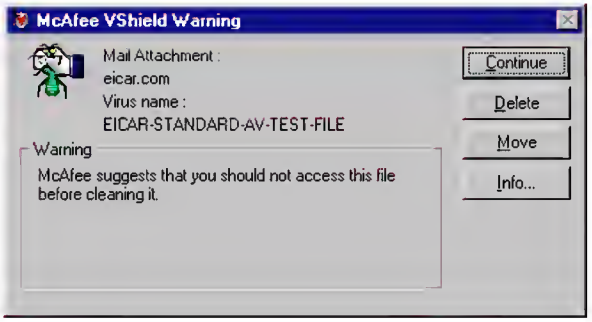

Figure 3-7. Download Scan response options

Click the button that corresponds to the response you want. Your choices are:

- **Continue.** Click this to tell VShield to take no action and to resume scanning. VShield will continue until it finds another virus on your system or until it finishes the scan operation. Normally, you would use this option to bypass files that you know do not have viruses, or if you plan to leave your computer unattended as you download e-mail or other files. VShield will note each incident in its log file.
- **Delete.** Click this to tell VShield to delete the infected file or e-mail attachment you received. By default, VShield notes the name of the infected file in its log file.
- **Move.** Click this to tell VShield to create a quarantine directory where it found the virus, then move the infected file to it. If you use a POP-3 or SMTP mail client, the quarantine folder will appear as a folder called INFECTED at the root level of your hard disk as soon as you download an infected file.
- **Info.** Click this to connect to the Network Associates Virus Information Library. This choice does not take any action against the virus. See "Viewing File and Virus Information" on page 70 for more details.

When you choose your action, VShield will implement it and add a notice to the top of the e-mail message that contained the infected attachment. The notice gives the file name of the infected attachment, identifies the name of the infecting virus, and describes the action VShield took in response.

Internet Filter module

This module looks for hostile Java classes or ActiveX controls whenever you visit a website or download files from the Internet. You can also use the module to block your browser from connecting to dangerous Internet sites. In its initial configuration, the module will ask you whenever it encounters a potentially harmful object whether you want to **Deny** the object access to your system or you want to **Continue** and allow the object access. It will offer you the same choice when you try to connect to a potentially dangerous website (Figure 3-8).

Figure 3-8. Internet Filter response options

Responding when VirusScan detects a virus

When you first install VirusScan and start a scan operation, the program will look at all files on your C: drive that are susceptible to virus infection. This provides you with a basic level of protection that you can extend by configuring VirusScan to suit your own needs. In its initial configuration, the program will prompt you for a response when it finds a virus (Figure 3-9).

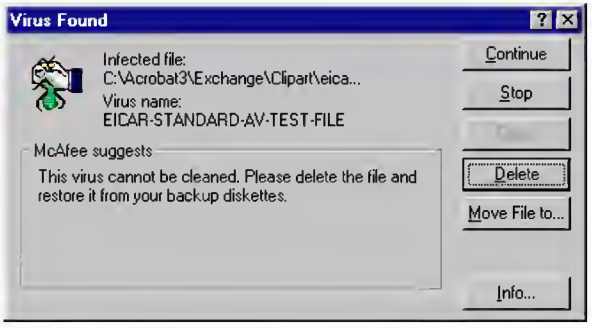

Figure 3-9. VirusScan response options

To respond to the infection, click one of the buttons shown. You can tell VirusScan to:

- **Continue.** Click this to proceed with the scan operation and have VirusScan list each infected file in the lower portion of its main window (Figure 3-10), record each detection in its log file, but take no other action to respond to the virus. Once VirusScan has finished examining your system, you can right-click each file listed in the main window, then choose an individual response from the shortcut menu that appears.

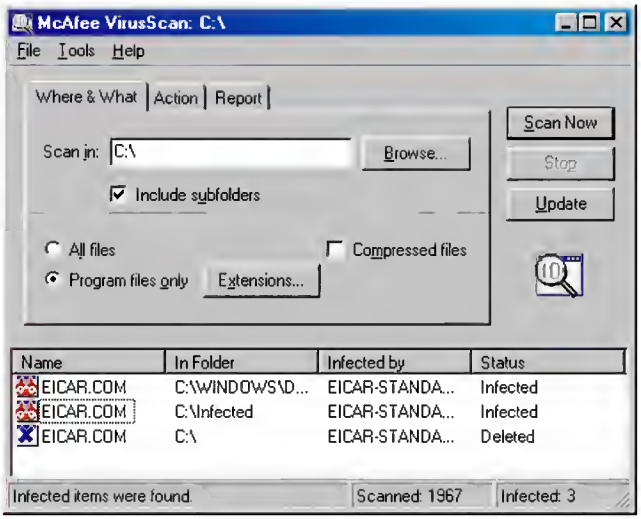

Figure 3-10. VirusScan main window

- **Stop.** Click this to stop the scan operation immediately. VirusScan will list the infected files it has already found in the lower portion of its main window (Figure 3-10) and record each detection in its log file, but it will take no other action to respond to the virus. Right-click each infected file listed in the main window, then choose an individual response from the shortcut menu that appears.

- **Clean.** Click this to have VirusScan try to remove the virus code from the infected file. If it cannot clean the file—either because it has no remover or because the virus has damaged the file beyond repair—it will record the incident in its log file and suggest alternative responses. In the example shown in Figure 3-9, VirusScan failed to clean the EICAR Test Virus—a mock "virus" written specifically to test whether your anti-virus software installed correctly. Here, **Clean** is not an available response option. In most cases, you should delete such files and restore them from backups.

- **Delete.** Click this to delete the file from your system immediately. By default, VirusScan will record the name of the infected file in its log so that you can restore the file from a backup copy.

- **Move file to.** Click this to open a dialog box that you can use to locate your quarantine folder, or another suitable folder. Once you have located the correct folder, click **OK** to transfer the file to that location.
- **Info.** Click this to connect to the Network Associates Virus Information Library. This choice does not take any action against the virus that VirusScan detected. See "Viewing File and Virus Information" on page 70 for more details.

Responding when E-Mail Scan detects a virus

VirusScan's E-Mail Scan program component lets you scan incoming Microsoft Exchange or Microsoft Outlook e-mail messages for viruses at your initiative. You can start it from within either e-mail client and use it to supplement VShield's continuous e-mail background scanning. E-Mail Scan also offers the ability to clean infected file attachments or stop the scan operation, a capability that complements VShield's continuous monitoring. In its initial configuration, E-Mail Scan will prompt you for a response when it finds a virus (Figure 3-11).

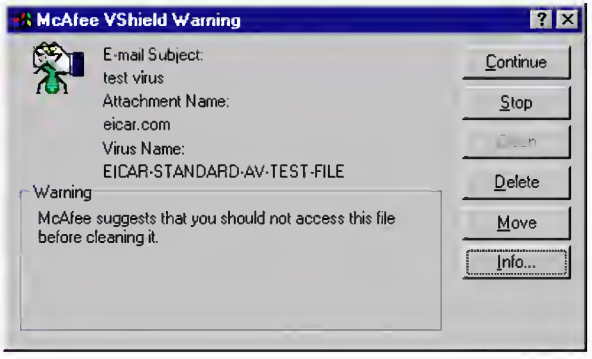

Figure 3-11. E-Mail Scan response options

To respond to the infection, click one of the buttons shown. You can tell E-Mail Scan to:

- **Continue.** E-Mail Scan will proceed with its scan operation, list each infected file it finds in the lower portion of its main window (Figure 3-12), and record each detection in its log file, but it will take no other action to respond to the virus. E-Mail Scan will continue until it finds another virus on your system or until it finishes the scan operation. Once it has finished examining your system, you can right-click each file listed in the main window, then choose an individual response from the shortcut menu that appears.
- **Stop.** E-Mail Scan will stop its scan operation immediately. It will list the infected files it has already found in the lower portion of its main window (Figure 3-12) and record each detection in its log file, but it will take no other action to respond to the virus. Right-click each infected file listed in the main window, then choose an individual response from the shortcut menu that appears.

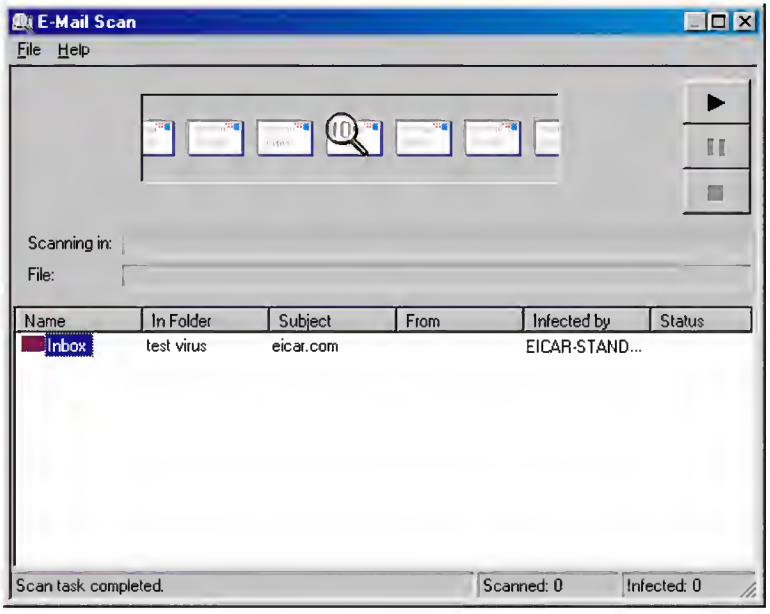

Figure 3-12. E-Mail Scan window

- **Clean.** E-Mail Scan will try to remove the virus code from the infected file. If it cannot clean the file—either because it has no remover or because the virus has damaged the file beyond repair—it will record the incident in its log file and suggest alternative responses. In the example shown in Figure 3-11, **Clean** is not an available response option. In most cases, you should delete such files and restore them from backups.

- **Delete.** E-Mail Scan will immediately delete the file from your system. By default, the program will record the name of the infected file in its log so that you can restore the file from a backup copy.
- **Move.** E-Mail Scan will open a dialog box that you can use to locate your quarantine folder, or another suitable folder. Once you have located the correct folder, click **OK** to transfer the file to that location.
- **Info.** E-Mail Scan will open a dialog box that displays information about the infecting virus or the infected file. This choice does not cause the program to take any action against the virus it detected. See "Viewing File and Virus Information" for more details.

Viewing File and Virus Information

Clicking **Info** in any of the virus response dialog boxes will connect you to the Network Associates online Virus Information Library, provided you have an Internet connection and web browsing software available on your computer (Figure 3-13).

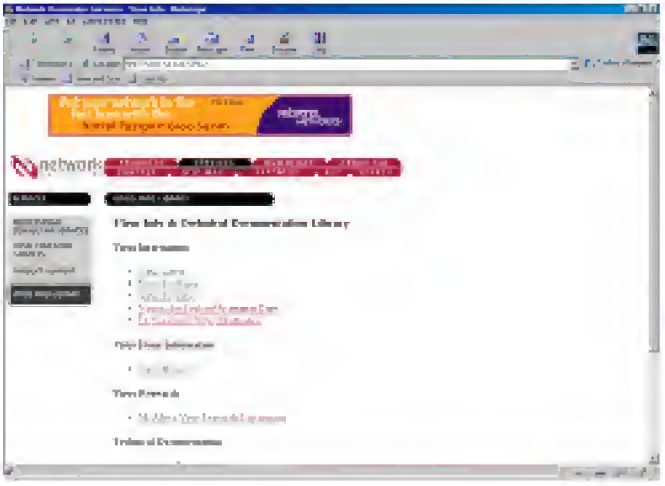

Figure 3-13. Online Virus Information Library

The Virus Information Library contains documents that give a detailed overview of each virus that VirusScan can detect or clean. That information includes how the virus infects and alters files, the sorts of payloads it deploys, how to recognize an infection, and other data. The Library also gives tips on preventing virus infection and removing viruses that VirusScan cannot remove from infected files.

If you choose **File Info** from the **File** menu in the VirusScan main window (see Figure 3-10 on page 67), or right-click a file listed either in the VirusScan main window or the E-Mail Scan window (see Figure 3-12 on page 69), then choose **File Info** from the shortcut menu that appears, VirusScan will open an Infected Item Information dialog box that names the file, lists its type and size in bytes, gives its creation and modification dates, and describes its attributes (see Figure 3-14 on page 71).

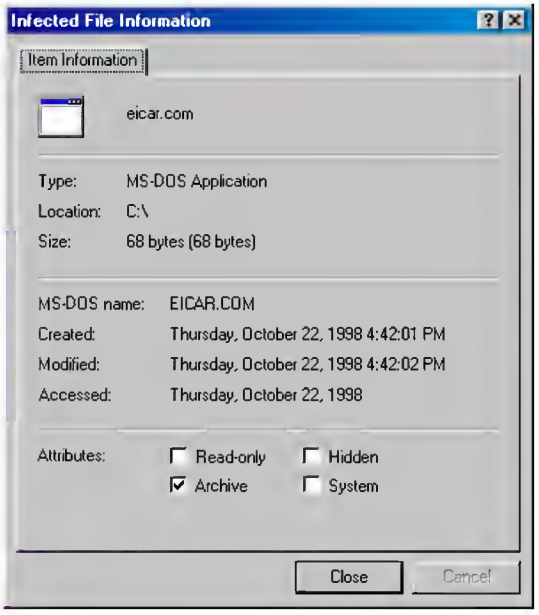

Figure 3-14. Infected File Information property page

Understanding false detections

A false detection occurs when VirusScan sends a virus alert message or makes a log file entry that identifies a virus where none actually exists. You are more likely to see false detections if you have anti-virus software from more than one vendor installed on your computer, because some anti-virus software stores the code signatures it uses for detection unprotected in memory.

The safest course to take when you see an alert message or log entry is to treat it as a genuine virus threat, and to take the appropriate steps to remove the virus from your system. If, however, you believe that VirusScan has generated a false detection—it has, for example, flagged a file as infected when you have used it safely for years—verify that you are not seeing one of these situations before you call Network Associates:

- **You have more than one anti-virus program running.** If so, VirusScan might detect unprotected code signatures that another program uses and report them as viruses. To avoid this problem, configure your computer to run only one anti-virus program, then shut the computer down and turn off the power. Wait a few seconds before you start the computer again so that the system can clear the other program's code signature strings from memory.
- **You have a BIOS chip with anti-virus features.** Some BIOS chips provide anti-virus features that can trigger false detections when VirusScan runs. Consult the user's guide for your computer to learn about how its anti-virus features work and how to disable them if necessary.
- **You have an older Hewlett-Packard or Zenith PC.** Some older models from these manufacturers modify the boot sectors on their hard disks each time they start up. VirusScan might detect these modifications as viruses, when they are not. Consult the user's guide for your computer to learn whether it uses self-modifying boot code. To solve the problem, use the command-line version of VirusScan to add validation information to the startup files themselves. This method does not save information about the boot sector or the master boot record.
- **You have copy-protected software.** Depending on the type of copy protection used, VirusScan might detect a virus in the boot sector or the master boot record on some floppy disks or other media.

If none of these situations apply, contact Network Associates technical support or send e-mail to AVresearch@nai.com with a detailed explanation of the problem you encountered.

Using VShield 4

What does VShield do?

VShield scans your system in the background, as you work with your files, in order to protect you from viruses borne on floppy disks, brought in from your network, embedded in file attachments that come with e-mail messages, or loaded into memory. It starts when you start your computer, and stays in memory until you shut down. VShield also includes technology that guards against hostile Java applets and ActiveX controls, and that keeps your computer from connecting to dangerous Internet sites. Secure password protection for your configuration options prevents others from making unauthorized changes.

Why use VShield?

VShield has unique capabilities that make it an integral part of VirusScan's comprehensive anti-virus security package. These include:

- **"On-access" scanning.** This means that VShield scans for viruses in files that you open, copy, save, or otherwise modify, and files that you read from or write to floppy disks. It therefore can detect and stop viruses as soon as they appear on your system. This gives you an extra measure of anti-virus protection between each scan operation that you perform.
- **Malicious object detection and blocking.** VShield can block harmful ActiveX and Java objects from gaining access to your system, before they pose a threat. VShield does this by scanning the hundreds of objects you download as you connect to the web or to other Internet sites, and the file attachments you receive with your e-mail. It compares these items against a current list of harmful objects that it maintains, and blocks those that could cause problems.
- **Internet site filtering.** VShield comes with a list of dangerous web- or Internet sites that pose a hazard to your system, usually in the form of downloadable malicious software. You can add any other site that you want to keep your browser software from connecting to, either by listing its Internet Protocol (IP) address or its domain name.
- **Automatic operation.** VShield integrates with a wide range of browser software and e-mail client applications based on Microsoft's Messaging Application Programming Interface (MAPI) standard. This allows VShield to log on to and scan your e-mail attachments for viruses before they ever reach your computer.

Which browsers and e-mail clients does VShield support?

VShield works seamlessly with many of the most popular web browsers and e-mail client software available for the Windows platform. To work with your browser, VShield requires no setup beyond what you have already done to connect your computer to the Internet. You must configure VShield, however, to work correctly with your e-mail client software. See See "Using the VShield configuration wizard" on page 75 or "Setting VShield properties" on page 81 to learn how to do the required setup.

Web browsers tested and known to work correctly with VShield are:

- Netscape Navigator v3.x
- Netscape Navigator v4.0.x (not including v4.0.6)
- Microsoft Internet Explorer v3.x
- Microsoft Internet Explorer v4.x

E-mail clients tested and known to work with VShield's Download Scan module are:

- Microsoft Outlook Express
- Qualcomm Eudora v3.x and v4.x
- Netscape Mail (included with most versions of Netscape Navigator and Netscape Communicator)
- America Online mail v3.0 and v4.0

In order to work with VShield's E-mail Scan module, you must use particular versions of Lotus cc:Mail, or your e-mail client software must support Microsoft's MAPI standard. Those clients tested and known to work correctly with the E-mail Scan module are:

- Microsoft Exchange v4.0, v5.0 and v5.5
- Microsoft Outlook 97 and Outlook 98
- Lotus cc:Mail v6.x and v7.x (not MAPI-compliant)
- cc:Mail v8.0 and v8.01 (MAPI-compliant version only)

Other MAPI-compliant client software will most likely work correctly with VShield, but Network Associates does not certify VShield compatibility with client software not listed above.

Using the VShield configuration wizard

After you install VirusScan and restart your computer, VShield loads into memory immediately and begins working with a default set of options that give you basic anti-virus protection. Unless you disable it or one of its modules—or stop it entirely—you never have to worry about starting VShield or scheduling scan tasks for it.

To ensure more than a minimal level of security, however, you should configure VShield to work with your e-mail client software and have it examine your Internet traffic closely for viruses and malicious software. VShield's configuration wizard can help you set up many of these options right away—you can then tailor the program to work better in your environment as you become more familiar with VShield and your system's susceptibility to harmful software.

To start the VShield configuration wizard, either:

- Start the VirusScan Scheduler, then select the VShield icon in the task list. Next, click in the Scheduler toolbar. To learn how to start and use the VirusScan Scheduler, see "Starting the VirusScan Scheduler" on page 166; or
- Locate the VShield icon in the Windows system tray, then click it with your right mouse button. Point to **Properties** in the shortcut menu that appears, then choose **System Scan**.

Either method opens the VShield Properties dialog box (Figure 4-1).

Figure 4-1. VShield Properties dialog box

Click **Wizard** in the lower-left corner of the dialog box to display the first configuration wizard panel (Figure 4-2).

VShield Configuration Wizard
Welcome to VShield Configuration Wizard!
This wizard will guide you through the steps to configure VShield on your machine.
VShield Configuration Wizard
Back
Next >
Cancel

Figure 4-2. VShield Configuration Wizard - Welcome panel

Click **Next>** to display the System Scan configuration panel (Figure 4-3).

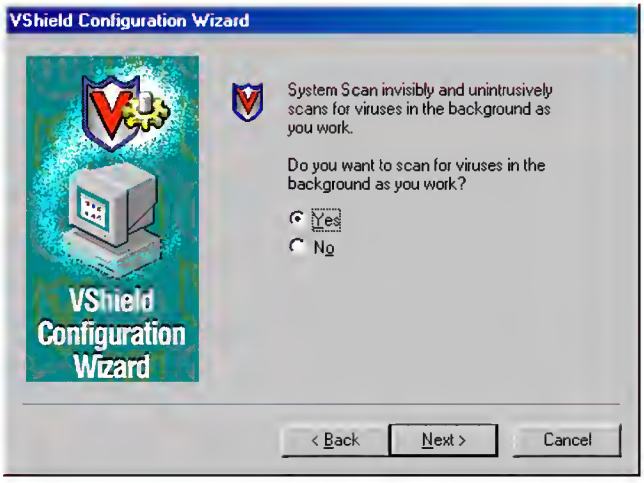
VShield Configuration Wizard
System Scan invisibly and unintrusively scans for viruses in the background as you work.
Do you want to scan for viruses in the background as you work?
Yes
No
VShield Configuration Wizard
< Back
Next >
Cancel

Figure 4-3. VShield Configuration Wizard - System Scan panel

Here you can tell VShield to look for viruses in files susceptible to infection whenever you open, run, copy, save or otherwise modify them. Susceptible files include various types of executable files and document files with embedded macros, such as Microsoft Office files. VShield will also scan files stored on floppy disks whenever you read from or write to them, or when you shut down your computer.

If it finds a virus, VShield will sound an alert and prompt you for a response. The program will also record its actions and summarize its current settings in a log file that you can review later.

To enable these functions, select **Yes**, then click **Next>**. Otherwise, select **No**, then click **Next>** to continue.

The E-mail Scan wizard panel will appear (Figure 4-4).

VShield Configuration Wizard
VShield Configuration Wizard
E-Mail scanner makes sure that all your mail attachments are free of viruses. Please select the type of e-mail client that you are using.
I do not use e-mail.
Enable Corporate Mail
MAPI compliant e-mail client.
(MAPI compliant clients are Microsoft Outlook, cc:Mail version 8)
cc:Mail version 6 / 7
Internet e-mail clients.
(AOL, Eudora, Netscape mail, Outlook Express)
< Back
Next >
Cancel

Figure 4-4. VShield Configuration Wizard - E-mail Scan panel

If you do not use e-mail or do not have an Internet connection, select the **I do not use e-mail** checkbox, then click **Next>** to continue. Otherwise, select the checkbox that corresponds to the type of e-mail client you use. Your choices are:

- **Enable Corporate Mail.** Select this checkbox if you use a proprietary e-mail system at work or in a networked environment. Most such systems use a central network server to receive and distribute mail that individual users send to each other from client applications. Such systems might send and receive mail from outside the network or from the Internet, but they usually do so through a "gateway" application run from the server.

  VShield supports corporate e-mail systems that fall into two general categories:

  - **MAPI-compliant e-mail client**. Select this button if you use an e-mail client that adheres to the MAPI standard. Examples of such clients include Microsoft Exchange, Microsoft Outlook, and version 8.0 or later of Lotus cc:Mail.

  - **Lotus cc:Mail.** Select this button if you use cc:Mail versions 6.x or 7.x, which use a proprietary Lotus protocol for sending and receiving mail.

- **Internet e-mail clients.** Select this checkbox if you use a Post Office Protocol (POP-3) or Simple Mail Transfer Protocol (SMTP) e-mail client that sends and receives standard Internet mail directly or through a dial-up connection. If you send and receive e-mail from home and use Netscape Mail, America Online, or such popular clients as Qualcomm's Eudora or Microsoft's Outlook, be sure to select this option.

When you have specified which e-mail system you use, click **Next>** to continue.

NOTE: If you use both types of mail systems, select both checkboxes. Note that VShield supports only one type of *corporate* e-mail system at a time, however. If you need to verify which e-mail system your office uses, check with your network administrator.

Be sure also to distinguish between Microsoft Outlook and Microsoft Outlook Express. Although the two programs share similar names, Outlook 97 and Outlook 98 are MAPI-compliant corporate e-mail systems, while Outlook Express sends and receives e-mail through the POP-3 and SMTP protocols. To learn more about these programs, consult your Microsoft documentation.

The next wizard panel sets options for VShield's Download Scan module (Figure 4-5).

VShield Configuration Wizard
Do you download files over the internet that you would like to have scanned for viruses?
Yes, do scan my downloaded files for viruses.
No, do not enable download scanning.
VShield Configuration Wizard
< Back
Next >
Cancel

Figure 4-5. VShield Configuration Wizard - Download Scan panel

To have VShield look for viruses in each file that you download from the Internet, select the **Yes, do scan my downloaded files for viruses** checkbox, then click **Next>** to continue. VShield will look for viruses in those files most susceptible to infection and will scan compressed files as you receive them.

Otherwise, select the **No, do not enable download scanning** checkbox, then click **Next>** to continue.

The next wizard panel sets options for VShield's Internet Filter module (see Figure 4-6 on page 80).

VShield Configuration Wizard
Would you like to protect your computer from hostile Internet applets and prevent access to unsafe websites?
Yes, enable hostile applet protection and access prevention to unsafe websites.
No, do not enable hostile applet protection and access prevention to unsafe websites.
VShield Configuration Wizard
< Back
Next >
Cancel

Figure 4-6. VShield Configuration Wizard - Internet Filter panel

Select **Yes, enable hostile applet protection and access prevention to unsafe websites**, then click **Next>** to have VShield block Java applets and ActiveX controls that can cause your system harm. This option will also keep your web browser from connecting to potentially dangerous web- or other Internet sites. VShield maintains a list of harmful objects and sites that it uses to check the sites you visit and the objects you encounter. If it finds a match, it can either block it automatically, or offer you the chance to allow or deny access.

To disable this function, select **No, do not enable hostile applet protection and access prevention to unsafe websites**, then click **Next>** to continue.

The final wizard panel summarizes the options you chose (Figure 4-7).

Figure 4-7. VShield Configuration Wizard - summary panel

If the summary list accurately reflects your choices, click **Finish** to save your changes and return to the VShield Properties dialog box. Otherwise, click **<Back** to change any options you chose, or **Cancel** to return to the VShield Properties dialog box without saving any of your changes.

Setting VShield properties

To ensure its optimal performance on your computer or in your network environment, VShield needs to know what you want it to scan, what you want it to do if it finds a virus or other malicious software, and how it should let you know when it has. You can use the configuration wizard to enable most of VShield's protective options, but if you want complete control over the program's performance and the ability to adapt it to your needs, choose your options in the VShield Properties dialog box.

The VShield Properties dialog box consists of a series of property pages that control the settings for each program module. To choose your options, click the icon for the appropriate program module, then click each tab in the VShield Properties dialog in turn.

To open the VShield Properties dialog box, either:

- Start the VirusScan Scheduler, then select the VShield icon in the task list. Next, click in the Scheduler toolbar. To learn how to start and use the VirusScan Scheduler, see "Starting the VirusScan Scheduler" on page 166; or

- Locate the VShield icon in the Windows system tray, then click it with your right mouse button. Point to **Properties** in the shortcut menu that appears, then choose **System Scan**.

Either method opens the VShield Properties dialog box (Figure 4-8).

Figure 4-8. System Scan Properties dialog box - Detection page

Configuring the System Scan module

VShield's System Scan module can check your system for viruses each time you open, run, save, or modify files on your hard disk, and each time you read from or write to a floppy disk. To choose your options, click the System Scan icon at the left side of the VShield Properties dialog box to display the property pages for this module. The next sections describe your options.

Choosing Detection options

VShield initially assumes that you want it to scan for viruses each time you work with any file susceptible to virus infection, whether on your hard disk or on floppy disks (see Figure 4-8 on page 82). Although these default options balance scan performance with security, your environment might require different settings.

To modify these settings, verify that the Enable System Scan checkbox is selected, then follow these steps:

1. Tell VShield when and where you want it to look for viruses. You can have it

   - **Scan files as you work with them.** Each time you open, copy, save, rename, or otherwise use files on your hard disk, virus code can execute and spread infections to other files. To prevent this, select any combination of the **Run**, **Copy**, **Create** and **Rename** checkboxes—selecting all options offers you the best security. VShield will delay each operation very slightly as it scans each file.

   - **Scan files on floppy disks.** Boot-sector viruses can hide in the boot blocks of any formatted floppy disk, then load into memory as soon as your computer reads your floppy drive. Select the **Access** checkbox to have VShield examine floppy disks each time your computer reads them. Select the **Shutdown** checkbox to have VShield scan any floppy disks that you leave in your drive as you shut down your computer. This ensures that no viruses can load when your computer reads your floppy drive at startup.

2. Specify the types of files you want VShield to examine. You can

   - **Scan compressed files.** Select the **Compressed files** checkbox to have System Scan look for viruses in files compressed with LZEXE and PKLite. Although it does give you better protection, scanning compressed files can increase the time it takes to run a scan operation.

   - **Choose file types for scanning.** Viruses ordinarily cannot infect data files or files that contain no executable code. You can, therefore, safely narrow the scope of your scan operations to those files most susceptible to virus infection in order to speed up scan operations. To do so, select the **Program files only** button. To see or designate the file name extensions VShield will examine, click **Extensions** to open the Program File Extensions dialog box (Figure 4-9).

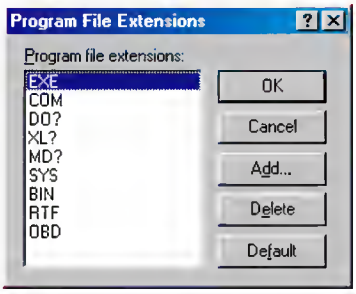

Figure 4-9. Program File Extensions dialog box

By default, VShield looks for viruses in files with the extensions .EXE, .COM, .DO?, .XL?, .MD?, .SYS, .BIN, .RTF, and .OBD. Files with .DO?, .XL?, .RTF, .MD?, and .OBD extensions are Microsoft Office files, all of which can harbor macro virus infections. The ? character is a wildcard that enables VShield to scan both document and template files.

NOTE: VShield's default program extension list differs from that used for VirusScan, because scanning .DLL and .VXD files—common files that Windows uses constantly—would slow down system performance dramatically. To have VShield scan these file types, add their extensions to the dialog box. As an alternative, consider running frequent VirusScan scan operations if you must scan these file types regularly.

- To add to the list, click **Add**, then type the extensions you want VShield to scan in the dialog box that appears.
- To remove an extension from the list, select it, then click **Delete**.
- Click **Default** to restore the list to its original form.

When you have finished, click **OK** to close the dialog box.

- **Scan all files.** To have VShield examine any file on your system that you use in any way, whatever its extension, select the **All files** button. This will slow your system down considerably, but will ensure that it is virus free.

3. Choose which types of heuristic scanning you want to enable. Click **Heuristics** to open the Heuristics Scan Settings dialog box (Figure 4-10).

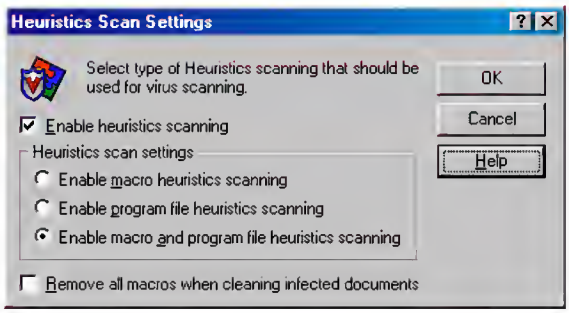
Heuristics Scan Settings
Select type of Heuristics scanning that should be used for virus scanning.
OK
Cancel
Help
Enable heuristics scanning
Heuristics scan settings
Enable macro heuristics scanning
Enable program file heuristics scanning
Enable macro and program file heuristics scanning
Remove all macros when cleaning infected documents

Figure 4-10. Macro Heuristics Scan Settings dialog box

Heuristic scan technology enables VShield to recognize new viruses based on their resemblance to similar viruses VShield already knows. To do this, the program looks for certain "virus-like" characteristics in the files you've asked it to scan. The presence of a sufficient number of these characteristics in a file leads VShield to identify the file as potentially infected with a new or previously unidentified virus.

Because VShield looks simultaneously for file characteristics that rule out the possibility of virus infection, it will rarely give you a false indication of a virus infection. Therefore, unless you know that the file does *not* contain a virus, you should treat "potential" infections with the same caution you would confirmed infections.

To activate heuristic scanning, follow these steps:

a. Select the **Enable heuristics scanning** checkbox. The remaining options in the dialog box activate.

b. Select the types of heuristic scanning you want VShield to use. Your choices are:

- **Enable macro heuristics scanning**. Choose this option to have VShield identify all Microsoft Word, Microsoft Excel, and other Microsoft Office files that have embedded macros, then compare the macro code to its virus signature database. VShield will identify exact matches with the virus name; code signatures that resemble existing viruses cause VShield to tell you it has found a potential macro virus.

- **Enable program file heuristics scanning.** Choose this option to have VShield locate new viruses in program files by examining their characteristics and comparing them against a list of known virus characteristics. VShield will identify files with a sufficient number of these characteristics as potential viruses.
- **Enable macro and program file heuristics scanning.** Choose this option to have VShield use both types of heuristic scanning. Network Associates recommends that you use this option for complete anti-virus protection.

c. Determine how you want to treat infected macro files. Select **Remove all macros when cleaning infected documents** to eliminate all infectable code from the document and leave only data. To try to remove only the virus code from the document's macros, leave this checkbox clear.

> **WARNING:** Use this feature with caution: removing all macros from a document can cause it to lose data or to become corrupted and unusable.

d. Click **OK** to save your settings and return to the VShield Properties dialog box.

4. Choose VShield management options. These options let you control your interaction with VShield. You can

- **Disable the System Scan module at will.** Select the **System Scan can be disabled** checkbox in order to have the option to disable this module. Note that Network Associates recommends that you leave System Scan enabled for maximum protection. Clearing this checkbox removes the disable command from VShield's shortcut menu and the disable button from the VShield Status dialog box.

> **TIP:** To ensure that nobody else who uses your computer will disable VShield, or to enforce an anti-virus security policy among VirusScan users on your network, clear this checkbox, then protect the settings with a password. This will keep other users from disabling VShield from VirusScan Scheduler, or from the VShield Properties dialog box. See "Configuring the Security module" on page 128 for details.

- **Display the VShield icon in the Windows system tray.** Select the **Show Icon in the Taskbar** checkbox to have VShield display this icon in the system tray. Double-clicking the icon opens the VShield Status dialog box. Right-clicking the icon displays a shortcut menu. See "Using VShield's shortcut menu" on page 132 and "Tracking VShield status information" on page 136 for more details.

5. Click the Action tab to choose additional VShield options. To save your changes without closing the System Scan Properties dialog box, click **Apply**. To save your changes and close the dialog box, click **OK**. To close the dialog box without saving your changes, click **Cancel**.

> **NOTE:** Clicking **Cancel** will not undo any changes you already saved by clicking **Apply**.

Choosing Action options

When VShield detects a virus, it can respond either by asking you what it should do with the infected file, or by automatically taking an action that you determine ahead of time. Use the Action property page to specify which response options you want VShield to give you when it finds a virus, or which actions you want it to take on its own.

Follow these steps:

1. Click the Action tab in the System Scan module to display the correct property page (Figure 4-11).

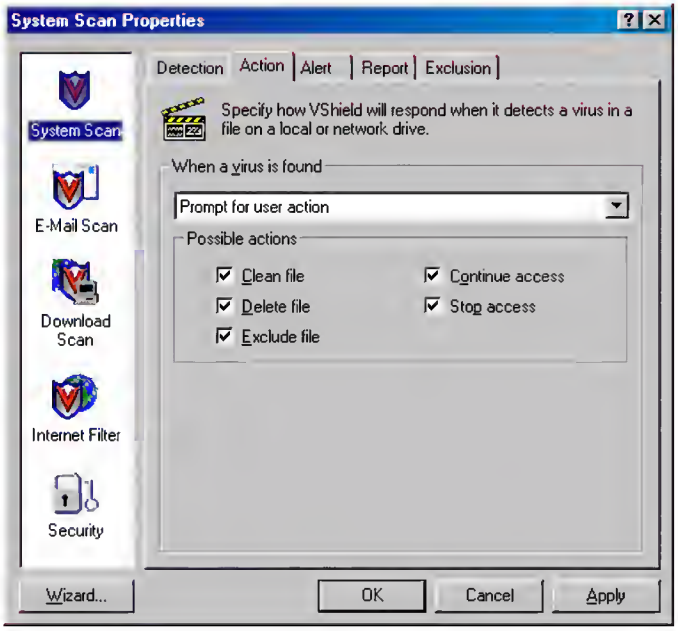

Figure 4-11. System Scan Properties dialog box - Action page

2. Choose a response from the **When a virus is found** list. The area immediately beneath the list will change to show you additional options for each choice.

Your choices are:

- **Prompt for user action.** Choose this response to have VShield ask you what to do when it finds a virus—the program will display an alert message and offer you a range of possible responses. Select the options you want to see in the alert message:
  - **Clean file.** This option tells VShield to try to remove the virus code from the infected file.
  - **Delete file.** This option tells VShield to delete the infected file immediately.
  - **Exclude file.** This option tells VShield not to scan the file from now on.
  - **Continue access.** This option tells VShield to allow you to continue working with the file and not take any other action. If you have its reporting options enabled, VShield records the incident in its log file. This option also causes VShield to display a full-screen alert instead of a dialog box when it finds a virus. See "Responding when VShield detects malicious software" on page 60 for details.
  - **Stop access.** This option tells VShield to deny you any access to the file, but not to take any other action. Denying access to the file prevents you from opening, saving, copying or renaming it. To continue, you must click **OK**. If you have activated its reporting feature, VShield records the incident.
- **Move infected files automatically**. Choose this response to have VShield move infected files to a quarantine directory as soon as it finds them. By default, VShield moves these files to a folder named INFECTED that it creates at the root level of the drive on which it found the virus. For example, if VShield found an infected file in T:\MY DOCUMENTS and you specified INFECTED as the quarantine directory, VShield would copy the file to T:\INFECTED.

  You can enter a different name and path in the text box provided, or click **Browse** to locate a suitable folder on your hard disk.
- **Clean infected files automatically.** Choose this response to tell VShield to remove the virus code from the infected file as soon as it finds it. If VShield cannot remove the virus, it will notify you in its message area and, if you have activated its reporting feature, will note the incident in its log file. See "Choosing Report options" on page 93 for details.
- **Delete infected files automatically.** Choose this response to have VShield delete every infected file it finds immediately. Be sure to enable its reporting feature to find out which files VShield deleted. You will need to restore deleted files from backup copies.

- **Deny access to infected files and continue.** Choose this response to have VShield to mark the file "off limits" and continue with its normal scanning operations. Choose this response only if you plan to leave your computer unattended for long periods. If you also activate VShield's reporting feature (see "Choosing Report options" on page 93 for details), the program will record the names of any viruses it finds and the names of infected files so that you can delete them at your next opportunity.

3. Click the Alert tab to choose additional VShield options. To save your changes without closing the System Scan Properties dialog box, click **Apply**. To save your changes and close the dialog box, click **OK**. To close the dialog box without saving your changes, click **Cancel**.

> **NOTE:** Clicking **Cancel** will not undo any changes you already saved by clicking **Apply**.

Choosing Alert options

Once you configure it with the response options you want, you can let VShield look for and remove viruses from your system automatically, as it finds them, with almost no further intervention. If, however, you want VShield to inform you immediately when it finds a virus so that you can take appropriate action, you can configure it to send an alert message to you or others in a variety of ways. Use the Alert property page to choose which alerting methods you want to use.

Follow these steps:

1. Click the Alert tab in the System Scan module to display the correct property page (Figure 4-12).

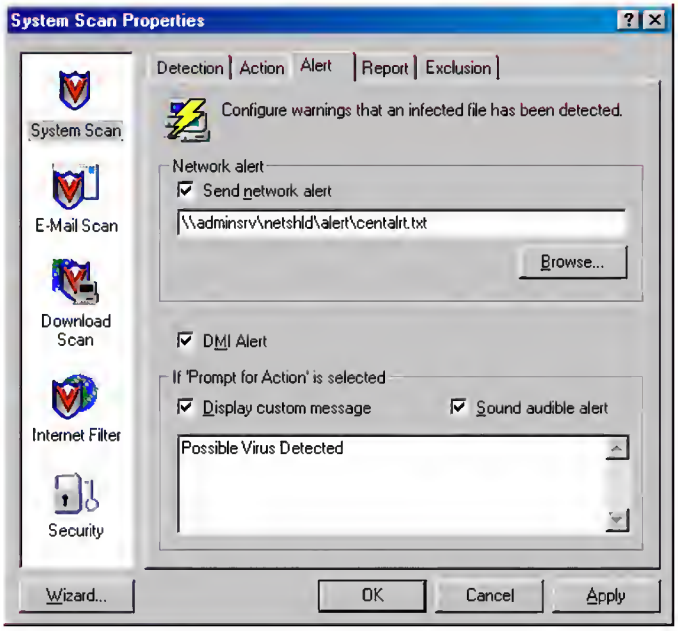

Figure 4-12. System Scan Properties dialog box - Alert page

2. To tell VShield to send an alert message to a server running NetShield, a Network Associates server-based anti-virus solution, select the **Send network alert** checkbox, then enter the path to the NetShield alert folder on your network, or click **Browse** to locate the correct folder.

   NOTE: The folder you choose must contain CENTALRT.TXT, the NetShield Centralized Alerting file. NetShield collects alert messages from VShield and other Network Associates software, then passes them to network administrators for action. To learn more about Centralized Alerting, see the NetShield *User's Guide*.

3. To have VShield send virus alert messages via the DMI Component Interface to desktop and network management applications running on your network, select the **DMI Alert** checkbox.

   NOTE: The Desktop Management Interface is a standard for communicating management requests and alert information between hardware and software components stored on or connected to desktop computers, and the applications used for managing them. To learn more about using this alert method, consult your network administrator.

4. If you chose **Prompt for user action** as your response in the Action page (see "Choosing Action options" on page 87 for details), you can also tell VShield to beep and display a custom message when it finds a virus. To do so, select the **Display custom message** checkbox, then enter the message you want to see in the text box provided—you can enter a message up to 225 characters in length. Next, select the **Sound audible alert** checkbox.

5. Click the Report tab to choose additional VShield options. To save your changes without closing the System Scan Properties dialog box, click **Apply**. To save your changes and close the dialog box, click **OK**. To close the dialog box without saving your changes, click **Cancel**.

> **NOTE:** Clicking **Cancel** will not undo any changes you already saved by clicking **Apply**.

Choosing Report options

VShield's System Scan module lists its current settings and summarizes all of the actions it takes during its scanning operations in a log file called VSHLOG.TXT. You can have VShield write its log to this file, or you can use any text editor to create a text file for it to use. You can then open and print the log file for later review from any text editor.

The VSHLOG.TXT file can serve as an important management tool for you to track virus activity on your system and to note which settings you used to detect and respond to the infections VShield found. You can also use the incident reports recorded in the file to determine which files you need to replace from backup copies, examine in quarantine, or delete from your computer. Use the Report property page to determine which information VShield will include in its log file.

To set VShield to record its actions in a log file, follow these steps:

1. Click the Report tab in the System Scan module to display the correct property page (Figure 4-13).

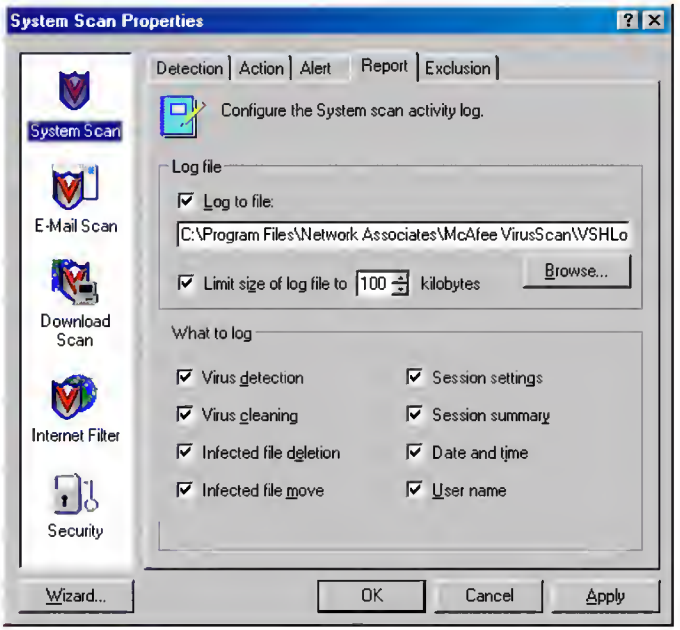

Figure 4-13. System Scan Properties dialog box - Report page

2. Select the **Log to file** checkbox.

By default, VShield writes log information to the file VSHLOG.TXT in the VirusScan program directory. You can enter a different name and path in the text box provided, or click **Browse** to locate a suitable file elsewhere on your hard disk or on your network.

3. To minimize the log file size, select the **Limit size of log file to** checkbox, then enter a value for the file size, in kilobytes, in the text box provided.

   Enter a value between 10KB and 999KB. By default, VShield limits the file size to 100KB. If the data in the log exceeds the file size you set, VShield erases the existing log and begins again from the point at which it left off.

4. Select the checkboxes that correspond to the information you want VShield to record in its log file. You can choose to record any of this information:

   - **Virus detection.** Select this checkbox to have VShield note the number of infected files it found during this scanning session.
   - **Virus cleaning.** Select this checkbox to have VShield note the number of infected files from which it removed the infecting virus.
   - **Infected file deletion.** Select this checkbox to have VShield note the number of infected files it deleted from your system.
   - **Infected file move.** Select this checkbox to have VShield note the number of infected files it moved to your quarantine directory.
   - **Session settings.** Select this checkbox to have VShield list the options you choose in the System Scan Properties dialog box for each scanning session.
   - **Session summary.** Select this checkbox to have VShield summarize its actions during each scanning session. Summary information includes the number of files VShield scanned, the number and type of viruses it detected, the number of files it moved or deleted, and other information.
   - **Date and time.** Select this checkbox to have VShield append the date and time to each log entry it records.
   - **User name.** Select this checkbox to have VShield append the name of the user logged in to your computer at the time it records each log entry.

5. Click the Exclusion tab to choose additional VShield options. To save your changes without closing the System Scan Properties dialog box, click **Apply**. To save your changes and close the dialog box, click **OK**. To close the dialog box without saving your changes, click **Cancel**.

NOTE: Clicking **Cancel** will not undo any changes you already saved by clicking **Apply**.

Choosing Exclusion options

Many of the files stored on your computer are not vulnerable to virus infection. Having VShield examine these files can take a long time and produce few results. You can speed up scan operations by telling VShield to look only at susceptible file types (see "Choosing Detection options" on page 82 for details), or you can tell VShield to ignore entire files or folders that you know cannot become infected.

Once you use VirusScan to scan your system thoroughly, you can tell VShield to ignore those files and folders that do not change or that are not normally vulnerable to virus infection. To keep VShield from scanning certain files and folders, follow these steps:

1. Click the Exclusion tab in the System Scan module to display the correct property page (Figure 4-14).

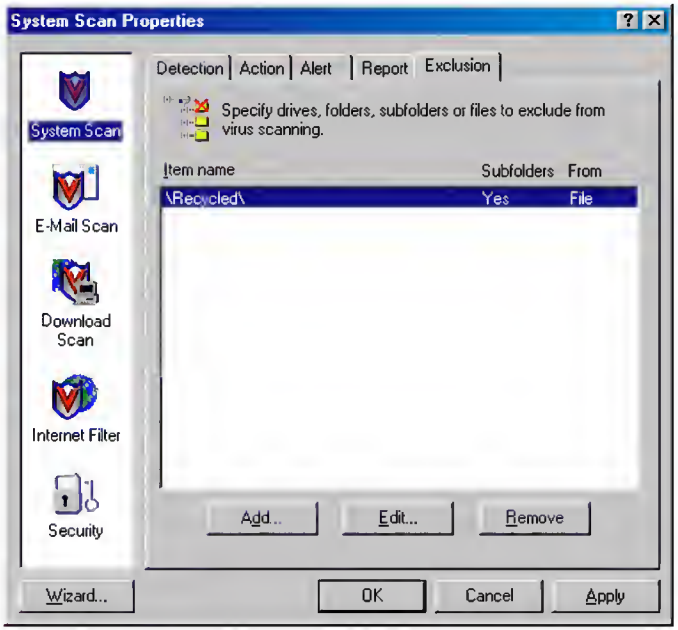

Figure 4-14. System Scan Properties dialog box - Exclusion page

The Exclusion page will initially list only your Recycle Bin. VShield excludes the Recycle Bin from scan operations because Windows will not run files stored there.

2. Specify the items you want to exclude. You can

- **Add files, folders or volumes to the exclusion list.** Click **Add** to open the Add Exclude Item dialog box (Figure 4-15).

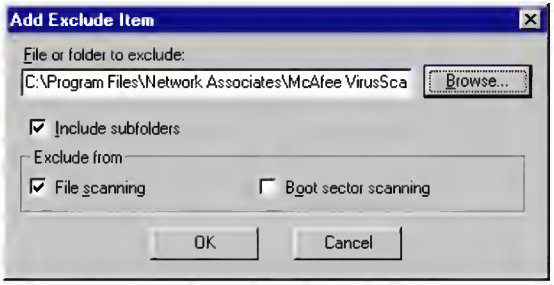

Figure 4-15. Add Exclude Item dialog box

  a. Type the volume, the path to the file, or the path to the folder that you want to exclude from scanning, or click **Browse** to locate a file or folder on your computer.

> **NOTE:** If you have chosen to move infected files to a quarantine folder automatically, VShield will not scan that folder.

  b. Select the **Include Subfolders** checkbox to exclude all subfolders within the folder you just specified.

  c. Select the **File scanning** checkbox to tell VShield not to look for file-infector viruses in the files or folders that you exclude.

  d. Select the **Boot sector scanning** checkbox to tell VShield not to look for boot-sector viruses in the files or folders you exclude. Use this option to exclude system files, such as COMMAND.COM, from scan operations.

> **WARNING:** Network Associates recommends that you do *not* exclude your system files from virus scanning.

  e. Click **OK** to save your changes and close the dialog box.

  f. Repeat steps a. through d. until you have listed all of the files and folders you do not want scanned.

- **Change the exclusion list.** To change the settings for an exclusion item, select it in the Exclusions list, then click **Edit** to open the Edit Exclude Item dialog box. Make the changes you need, then click **OK** to close the dialog box.

- **Remove an item from the list.** To delete an exclusion item, select it in the list, then click **Remove**. VShield will then scan this file or folder during its next scanning operation.

3. Click a different tab to change any of your System Scan settings, or click one of the icons along the side of the System Scan Properties dialog box to choose options for a different module.

   To save your changes in the System Scan module without closing its dialog box, click **Apply**. To save your changes and close the dialog box, click **OK**. To close the dialog box without saving your changes, click **Cancel**.

> **NOTE:** Clicking **Cancel** will not undo any changes you already saved by clicking **Apply**.

Configuring the E-mail Scan module

VShield's E-mail Scan module looks for viruses in files attached to e-mail messages you receive via a corporate e-mail system such as Microsoft Exchange, Microsoft Outlook, or Lotus cc:Mail, or via POP-3 or SMTP e-mail client programs such as Eudora, Netscape Mail, or Microsoft Outlook Express. VShield concentrates on the file attachments included with your e-mail, as the messages themselves, with very rare exceptions, are not normally vulnerable to infection. Because it can scan e-mail as soon as it appears in on your mail server or on your desktop, VShield can intercept viruses before they ever have a chance to spread.

To choose your options, click the E-mail Scan icon at the left side of the VShield Properties dialog box to display the property pages for this module. The next sections describe your options.

Choosing Detection options

VShield does not enable the E-mail Scan module by default, unless you've already used its configuration wizard to choose your options, because it needs to know which e-mail system you use.

To activate and configure e-mail scanning, follow these steps:

1. Select the **Enable Scanning of e-mail attachments** checkbox.

   The options in the rest of the property page activate (Figure 4-16).

Figure 4-16. E-mail Scan Properties dialog box - Detection page

2. Select the type of e-mail system you use. Your options are:

   - **Enable Corporate Mail.** Select this checkbox to have VShield scan mail attachments you receive via a mail system that runs within your office network. Usually such systems use a proprietary mail protocol and have a central mail server to which you send mail for delivery. Often such systems send and receive Internet mail, but they usually do so through a gateway application. The E-mail Scan module supports two types of corporate e-mail systems:

     – **Microsoft Exchange (MAPI).** Select this button if you use an e-mail system that sends and receives mail via Microsoft's Messaging Application Programming Interface (MAPI), a Windows mail protocol. Examples include Microsoft Exchange, Microsoft Outlook 97 and Outlook 98, Lotus cc:Mail 8.0, and cc:Mail 8.01.

     – **Lotus cc:Mail.** Select this button if you use cc:Mail 6.x or 7.x. These systems use a proprietary Lotus protocol to send and receive e-mail. You can also install cc:Mail version 8.0 or later so that it uses the same protocol as earlier cc:Mail versions. To verify which system you use, check with your network administrator.

     NOTE: To see the **Lotus cc:Mail** option, you must have used VirusScan's Custom Installation option to install VirusScan's cc:Mail scanner component. See Chapter 2, page 38 for details. You can select only one *corporate* e-mail system at a time, but you can have VShield scan all attachments that arrive via both corporate and Internet e-mail systems, if you use both.

   - **Internet Mail (Requires Download Scan).** Select this checkbox to have VShield scan Internet mail attachments that you send and receive via the Post Office Protocol (POP-3) or the Simple Mail Transfer Protocol (SMTP). Choose this option if you work from home or through a dial-up Internet service provider with such software as Qualcomm's Eudora Pro, Microsoft's Outlook Express, or Netscape Mail.

     IMPORTANT: Because you receive Internet mail and other files that you download from websites and other sources through the same "pipe," VShield uses the detection, action, alerting and reporting options you set in the Download Scan module to determine how to respond to incoming Internet mail. To scan Internet mail attachments, therefore, you must also enable the Download Scan module and use those property pages to choose the settings you want.

3. Tell VShield which mail sources it should monitor.

   - If you chose **Microsoft Mail (MAPI)** as your corporate e-mail system, your choices are:

     – **All new mail.** Select this button to have VShield look for viruses in files attached to each e-mail message as it arrives in your MAPI mailbox or via other MAPI services. Choose this option if you receive e-mail from more than one source—via your corporate e-mail system and a POP-3 or SMTP client, for instance—or if your mail system delivers to more than one mailbox.

     IMPORTANT: Because this option tells VShield to scan file attachments only in new e-mail messages, it will not find a virus in mail messages you already have stored on your computer or mail server. To ensure complete protection, run a full e-mail scan operation with VirusScan's E-Mail Scan component. See Chapter 7, "Using Specialized Scanning Tools," for details.

     – **Select Folder.** Select this button to designate a particular folder for VShield to scan. Choose this option if your e-mail system delivers your messages to a particular location on a mail server or on your computer. Next, click **Browse** to open a dialog box you can use to locate the folder you want VShield to watch.

     If you have already logged on to your e-mail system, the dialog box will show you available mailboxes and other folders for that system. If you have not logged in to your mail system, VShield will try to use your default MAPI profile to do so. Choose the folder you want VShield to scan, then click **OK** to close the dialog box.

   - If you chose **Lotus cc:Mail** as your corporate e-mail system, you'll need to tell VShield how often to scan your cc:Mail Inbox (Figure 4-17).

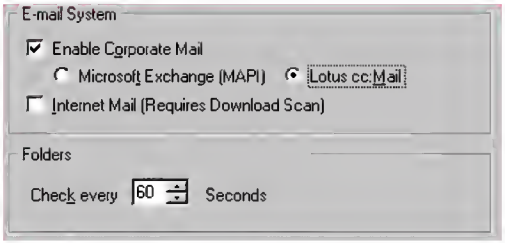

Figure 4-17. Detection page with cc:Mail option chosen

In the **Folders** area, enter the number of seconds VShield should wait before it looks for viruses. By default, it checks once every minute. Be sure to set an interval shorter than the interval you set to receive your e-mail so that VShield has an opportunity to detect any viruses before they reach your computer.

4. Specify the types of e-mail attachments you want VShield to examine. You can

   - **Scan compressed files.** Select the **Compressed files** checkbox to have E-Mail Scan look for viruses in files compressed with these formats: .??_, .CAB, LZEXE, LZH, PKLite, .TD0, and .ZIP. Although it does give you better protection, scanning compressed files can lengthen each operation, especially when you must process a large volume of mail.

   - **Choose file types for scanning.** Viruses ordinarily cannot infect data files or files that contain no executable code. You can, therefore, safely narrow the scope of your scan operations to those files most susceptible to virus infection. This speeds up scan operations when you have a large volume of mail to process.

     To do so, select the **Program files only** button. To see or designate the file name extensions VShield will examine, click **Extensions** to open the Program File Extensions dialog box (Figure 4-18).

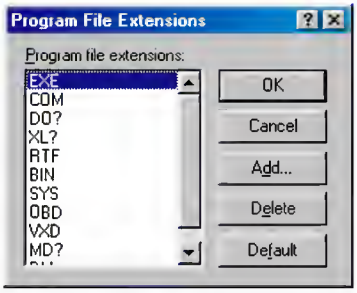

Figure 4-18. Program File Extensions dialog box

By default, VShield looks for viruses in files with the extensions .EXE, .COM, .DO?, .XL?, .RTF, .BIN, .SYS, .OBD,.VXD, .MD?, and .DLL. Files with .DO?, .XL?, .RTF, .MD?, and .OBD extensions are Microsoft Office files, all of which can harbor macro virus infections. The ? character is a wildcard that enables VShield to scan both document and template files.

- To add to the list, click **Add**, then type the extensions you want VShield to scan in the dialog box that appears.
- To remove an extension from the list, select it, then click **Delete**.
- Click **Default** to restore the list to its original form.

When you have finished, click **OK** to close the dialog box.

- **Scan all attachments.** To have VShield examine any attachment that arrives with any e-mail message, whatever its extension, select the **All attachments** button. This may slow e-mail processing down if you receive a large volume of e-mail, but it will ensure that your mail is virus free.

5. Click the Action tab to choose additional VShield options. To save your changes without closing the E-mail Scan Properties dialog box, click **Apply**. To save your changes and close the dialog box, click **OK**. To close the dialog box without saving your changes, click **Cancel**.

> **NOTE:** Clicking **Cancel** will not undo any changes you already saved by clicking **Apply**.

Choosing Action options

When VShield detects a virus in an e-mail attachment, it can respond either by asking you what it should do with the infected file, or by automatically taking an action that you determine ahead of time. Use the Action property page to specify which response options you want VShield to give you when it finds a virus, or which actions you want it to take on its own.

Follow these steps:

1. Click the Action tab in the E-mail Scan module to display the correct property page (Figure 4-19).

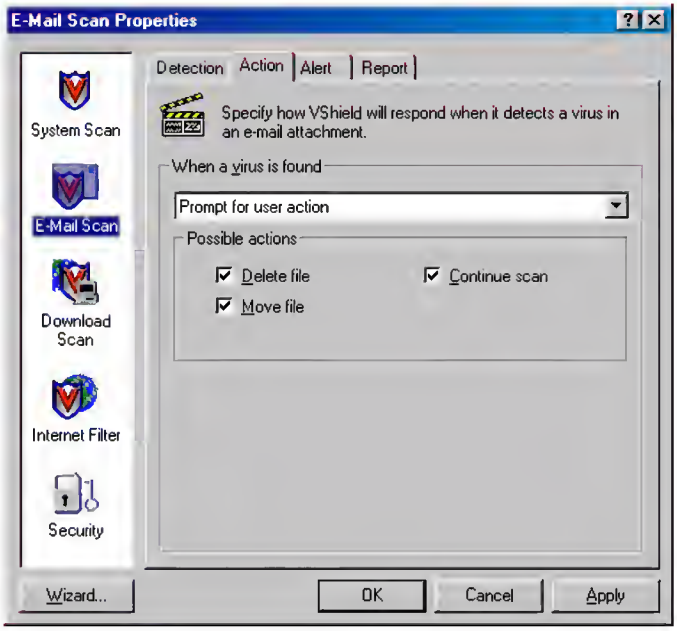

Figure 4-19. E-mail Scan Properties dialog box - Action page

2. Choose a response from the **When a virus is found** list. The area beneath the list will change to show you additional options for each response. Your choices are:

   - **Prompt for user action.** Choose this response if you want VShield to ask you what to do when it finds a virus—the program will display an alert message and offer you a range of possible responses. Select the options you want to see in the alert message :

     – **Delete file.** This option tells VShield to delete the infected attachment immediately. VShield will, however, preserve the e-mail message it came in.

     – **Move file.** This option tells VShield to move the infected file to a pre-selected quarantine directory.

     – **Continue scan.** This option tells VShield to continue with its scan, but not take any other actions. If you have its reporting options enabled, VShield records the incident in its log file.

   - **Move infected files to a folder**. Choose this response to have VShield move infected files to a quarantine directory as soon as it finds them. By default, VShield moves these files to a folder named INFECTED.

If you use a corporate e-mail system, VShield will create the INFECTED folder on the network mail server. You cannot designate a different folder or change the folder's name. Depending on the access you have to your mail server through your e-mail client, however, you might be able to see or delete the file in that folder.

If you use an Internet mail client, VShield will create the INFECTED folder at the root level of the drive to which you download your mail. For example, if your mail client's "in box" sits on your D: drive and VShield finds an infected attachment in your e-mail, it will create the directory D:\INFECTED and copy the file to it.

You can change the name and location of the folder into which VShield deposits infected Internet mail, but to do so, you must switch to the Download Scan module and click the Action tab there. See "Choosing Action options" on page 112 for details.

- **Delete infected files.** Choose this response to have VShield delete every infected file it detects immediately. Be sure to enable its reporting feature so that you have a record of which files VShield deleted. You will need to restore deleted files from backup copies. See "Choosing Report options" on page 108 for details.
- **Continue scanning.** Choose this response to have VShield continue scanning without taking any action against the virus it finds. If you also activate the VShield reporting feature (see "Choosing Report options" on page 108 for details), the program will record the names of any viruses it finds and the names of infected files so that you can delete them at your next opportunity.

3. Click the Alert tab to choose additional VShield options. To save your changes without closing the E-mail Scan Properties dialog box, click **Apply**. To save your changes and close the dialog box, click **OK**. To close the dialog box without saving your changes, click **Cancel**.

> **NOTE:** Clicking **Cancel** will not undo any changes you already saved by clicking **Apply**.

Choosing Alert options

Once you configure it with the response options you want, you can let VShield look for and remove viruses from your incoming e-mail automatically, as it finds them, with almost no further intervention. If, however, you want VShield to inform you immediately when it finds a virus so that you can take appropriate action, you can configure it to send an alert message to you and to others in a variety of ways. Use the Alerts property page to choose which alerting methods you want to use.

Follow these steps:

1. Click the Alert tab in the E-mail Scan module to display the correct property page (Figure 4-20).

Figure 4-20. E-mail Scan Properties dialog box - Alert page

2. To tell VShield to send an alert message to a server running NetShield, a Network Associates server-based anti-virus solution, select the **Send network alert** checkbox, then enter the path to the NetShield alert folder on your network, or click **Browse** to locate the correct folder.

> **NOTE:** The folder you choose must contain CENTALRT.TXT, the NetShield Centralized Alerting file. NetShield collects alert messages from VShield and other Network Associates software, then passes them to network administrators for action. To learn more about Centralized Alerting, see the NetShield *User's Guide*.

3. To send an alert message as a reply to the person who sent you the infected e-mail attachment, select the **Return reply mail to sender** checkbox. You can then compose a standard reply to send. Follow these steps:

   a. Click **Configure** to open a standard mail message form.

b. Fill in the subject line, then add any comments you want to make in the body of the message, below a standard infection notice that VShield will supply. You may add up to 1024 characters of text.

c. To send a copy of this message to someone else, enter an e-mail address in the text box labeled **Cc:**, or click **Cc:** to choose a recipient from your mail system's user directory or address book.

> **NOTE:** To find an e-mail address in your mail system's user directory, you must store address information in a MAPI-compliant user directory, database, or address book, or in an equivalent Lotus cc:Mail directory. If you have not yet logged onto your e-mail system, VShield tries to use your default MAPI profile to log onto MAPI-compliant mail systems, or asks you to supply a user name, password and path to your Lotus cc:Mail mailbox. Enter the information VShield requires, then click **OK** to continue.

d. Click **OK** to save the message.

Whenever it detects a virus, VShield will send a copy of this message to each person who sends you e-mail with an infected attachment. It fills in the recipient's address with information found in the original message header, and identifies the virus and the affected file in the area immediately below the subject line. If you have activated its report feature, VShield also logs each instance when it sends an alert message.

4. To send an e-mail message to warn others about an infected attachment, select the **Send alert mail to user** checkbox. You can then compose a standard reply to send to one or more recipients—a network administrator, for example—each time VShield detects an infected e-mail attachment. Follow these steps:

   a. Click **Configure** to open a standard mail message form.

   b. Enter an e-mail address in the text box labeled **To:**, or click **To:** to choose a recipient from your mail system's user directory or address book. Repeat the process in the text box labeled **Cc:** to send a copy of the message to someone else.

> **NOTE:** To find an e-mail address in your mail system's user directory, you must store address information in a MAPI-compliant user directory, database, or address book, or in an equivalent Lotus cc:Mail directory. If you have not yet logged onto your e-mail system, VShield tries to use your default MAPI profile to log onto MAPI-compliant mail systems, or asks you to supply a user name, password and path to your Lotus cc:Mail mailbox. Enter the information VShield requires, then click **OK** to continue.

c. Fill in the subject line, then add any comments you want to make in the body of the message below the infection notice. You may add up to 1024 characters of text.

d. Click **OK** to save the message.

Whenever it detects a virus, VShield sends a copy of this message to each of the addresses that you entered in Step b. It adds information to identify the virus and the affected file in the area immediately below the subject line. If you have activated its report feature, VShield also logs each instance when it sends an alert message.

5. To have VShield send virus alert messages via the DMI Component Interface to desktop and network management applications running on your network, select the **DMI Alert** checkbox.

> **NOTE:** The Desktop Management Interface is a standard for communicating management requests and alert information between hardware and software components stored on or connected to desktop computers, and the applications used for managing them. To learn more about using this alert method, consult your network administrator.

6. If you chose **Prompt for user action** as your response in the Action page (see "Choosing Action options" on page 102 for details), you can also tell VShield to beep and display a custom message when it finds a virus. To do so, select the **Display custom message** checkbox, then enter the message you want to see in the text box provided—you can enter a message up to 225 characters in length. Next, select the **Sound audible alert** checkbox.

7. Click the Report tab to choose additional VShield options. To save your changes without closing the E-mail Scan Properties dialog box, click **Apply**. To save your changes and close the dialog box, click **OK**. To close the dialog box without saving your changes, click **Cancel**.

> **NOTE:** Clicking **Cancel** will not undo any changes you already saved by clicking **Apply**.

Choosing Report options

VShield's E-mail Scan module lists its current settings and summarizes all of the actions it takes during its scanning operations in a log file called WEBEMAIL.TXT. You can have VShield write its log to this file, or you can use any text editor to create a text file for it to use. You can then open and print the log file for later review from any text editor.

The WEBEMAIL.TXT file can serve as an important management tool for you to track virus activity on your system and to note which settings you used to detect and respond to the infections VShield found. You can also use the incident reports recorded in the file to determine which files you need to replace from backup copies, examine in quarantine, or delete from your computer. Use the Report property page to determine which information VShield will include in its log file.

To set VShield to record its actions in a log file, follow these steps:

1. Click the Report tab in the E-mail Scan module to display the correct property page (see Figure 4-21 on page 108).

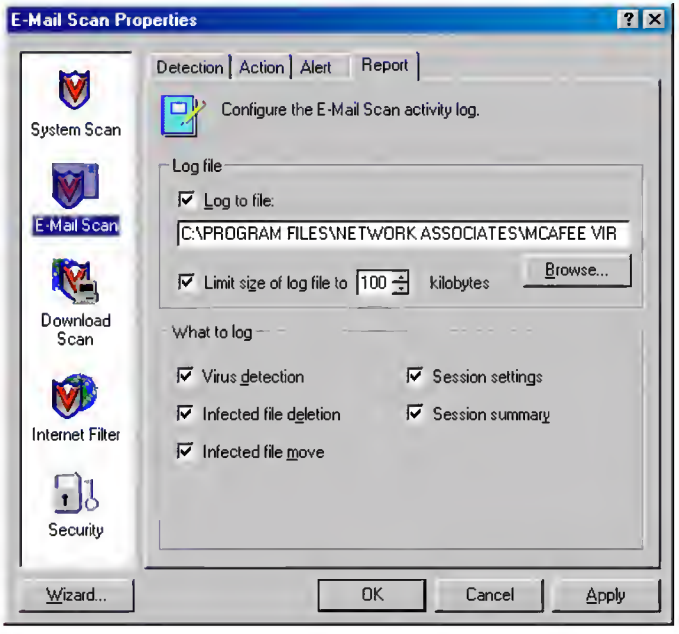

Figure 4-21. E-mail Scan Properties dialog box - Report page

2. Select the **Log to file** checkbox.

   By default, VShield writes log information to the file WEBEMAIL.TXT in the VirusScan program directory. you can enter a different name and path in the text box provided, or click **Browse** to locate a suitable file elsewhere on your hard disk or on your network.

3. To minimize the log file size, select the **Limit size of log file to** checkbox, then enter a value for the file size, in kilobytes, in the text box provided.

   Enter a value between 10KB and 999KB. By default, VShield limits the file size to 100KB. If the data in the log exceeds the file size you set, VShield erases the existing log and begins again from the point at which it left off.

4. Select the checkboxes that correspond to the information you want VShield to record in its log file. You can choose to record this information:

   - **Virus detection.** Select this checkbox to have VShield note the number of infected files it found as it checked your e-mail.
   - **Infected file deletion.** Select this checkbox to have VShield note the number of infected files it deleted as it checked your e-mail.
   - **Infected file move.** Select this checkbox to have VShield note the number of infected files it moved to your quarantine directory.
   - **Session settings.** Select this checkbox to have VShield list the options you choose in the E-mail Scan Properties dialog box for each scanning session.
   - **Session summary.** Select this checkbox to have VShield summarize its actions during each scanning session. Summary information includes the number of files VShield scanned, the number and type of viruses it detected, the number of files it moved or deleted, and other information.

5. Click a different tab to change any of your E-mail Scan settings, or click one of the icons along the side of the E-mail Scan Properties dialog box to choose options for a different module.

   To save your changes in the E-mail Scan module without closing its dialog box, click **Apply**. To save your changes and close the dialog box, click **OK**. To close the dialog box without saving your changes, click **Cancel**.

   ☐ **NOTE:** Clicking **Cancel** will not undo any changes you already saved by clicking **Apply**.

Configuring the Download Scan module

VShield's Download Scan module can check files you download from the Internet as you visit websites, FTP sites, and other Internet sites. This module is also where you set the options you want to use to respond to infected e-mail attachments you receive via POP-3 or SMTP e-mail client programs such as Eudora, Netscape Mail, or Microsoft Outlook Express. To activate this function, you must also choose an appropriate mail system in the E-mail Scan module's Detection page. See "Choosing Detection options" on page 97 for details.

To set VShield to scan files you download, click the Download Scan icon at the left side of the VShield Properties dialog box to display the property pages for this module. The next sections describe your options.

Choosing Detection options

VShield initially assumes that you want it to scan for viruses each time you download any file susceptible to virus infection from the Internet (see Figure 4-22 on page 110). These default options provide excellent security, but your environment might require different settings.

Figure 4-22. Download Scan Properties dialog box - Detection page

To modify these settings, verify that the Enable Internet Download Scanning checkbox is selected, then follow these steps:

1. Specify the types of files you want VShield to examine. You can

   - **Choose file types for scanning.** Viruses ordinarily cannot infect data files or files that contain no executable code. You can, therefore, safely narrow the scope of your scan operations to those files most susceptible to virus infection in order to speed up file downloading, particularly with large files or a large group of files. To do so, select the **Program files only** button. To see or designate the file name extensions VShield will examine, click **Extensions** to open the Program File Extensions dialog box (Figure 4-23).

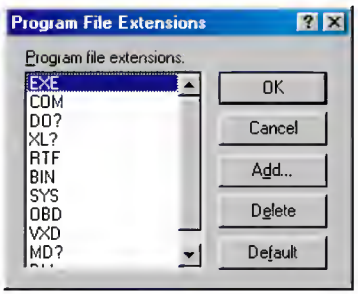

Figure 4-23. Program File Extensions dialog box

   By default, VShield looks for viruses in files with the extensions .EXE, .COM, .DO?, .XL?, .RTF, .BIN, .SYS, .OBD,.VXD, .MD?, and .DLL. Files with .DO?, .XL?, .RTF, .MD?, and .OBD extensions are Microsoft Office files, all of which can harbor macro virus infections. The ? character is a wildcard that enables VShield to scan both document and template files.

   - To add to the list, click **Add**, then type the extensions you want VShield to scan in the dialog box that appears.
   - To remove an extension from the list, select it, then click **Delete**.
   - Click **Default** to restore the list to its original form.

   When you have finished, click **OK** to close the dialog box.

   - **Scan all files.** To have VShield examine every file that you download, whatever its extension, select the **All files** button. This might slow download operations, but will ensure that your system remains virus free.

- **Scan compressed files.** Select the **Compressed files** checkbox to have Download Scan look for viruses in files compressed with these formats: .??_, .CAB, LZEXE, LZH, PKLite, .TD0, and .ZIP. Although it does give you better protection, scanning compressed files as you download them can increase download time.

2. Click the Action tab to choose additional VShield options. To save your changes without closing the Download Scan Properties dialog box, click **Apply**. To save your changes and close the dialog box, click **OK**. To close the dialog box without saving your changes, click **Cancel**.

> **NOTE:** Clicking **Cancel** will not undo any changes you already saved by clicking **Apply**.

Choosing Action options

When VShield detects a virus, it can respond either by asking you what it should do with the infected file, or by automatically taking an action that you determine ahead of time. Use the Action property page to specify which response options you want VShield to give you when it finds a virus, or which actions you want it to take on its own.

Follow these steps:

1. Click the Action tab in the Download Scan module to display the correct property page (Figure 4-24).

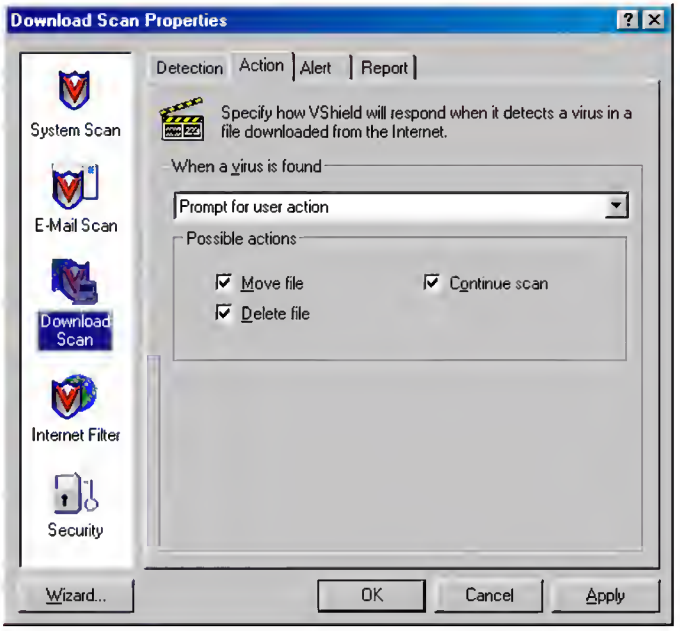

Figure 4-24. Download Scan Properties dialog box - Action page

2. Choose a response from the **When a virus is found** list. The area immediately beneath the list will change to show you additional options for each choice. Your choices are:

   - **Prompt for user action.** Choose this response to have VShield ask you what to do when it finds a virus—the program will display an alert message and offer you a range of possible responses. Select the options you want to see in the alert message:

     – **Move file.** This option tells VShield to move the infected file to a quarantine directory that you designate.

     – **Delete file.** This option tells VShield to delete the infected file immediately.

     – **Continue scan.** This option tells VShield to continue with its scan, but not take any other actions. If you have its reporting options enabled, VShield records the incident in its log file.

- **Move infected files to a folder**. Choose this response to have VShield move infected files to a quarantine directory as soon as it finds them. By default, VShield moves these files to a folder named INFECTED that it creates at the root level of the hard disk onto which you save the files that you download.

  For example, if VShield found a virus in a file you downloaded to E:\MY DOWNLOADS and you specified INFECTED as the quarantine directory, VShield would copy the file to E:\INFECTED.

  You can enter a different name and path in the text box provided, or click **Browse** to locate a suitable folder on your hard disk.

- **Delete infected files.** Choose this response to have VShield delete every infected file you download. Be sure to enable its reporting feature so that you have a record of which files VShield deleted.

- **Continue scanning.** Choose this response to have VShield continue scanning without taking any action against any virus it detects. If you also activate the VShield reporting feature (see "Choosing Report options" on page 116 for details), the program will record the names of any viruses it finds and the names of infected files so that you can delete them at your next opportunity.

3. Click the Alert tab to choose additional VShield options. To save your changes without closing the Download Scan Properties dialog box, click **Apply**. To save your changes and close the dialog box, click **OK**. To close the dialog box without saving your changes, click **Cancel**.

> **NOTE:** Clicking **Cancel** will not undo any changes you already saved by clicking **Apply**.

Choosing Alert options

Once you configure it with the response options you want, you can let VShield look for and remove viruses as it detects them in files you download, with almost no further intervention. If, however, you want VShield to inform you immediately when it finds a virus so that you can take appropriate action, you can configure it to send an alert message to you or to others in a variety of ways. Use the Alert property page to choose which alerting methods you want to use.

Follow these steps:

1. Click the Alert tab in the Download Scan module to display the correct property page (see Figure 4-25 on page 115).

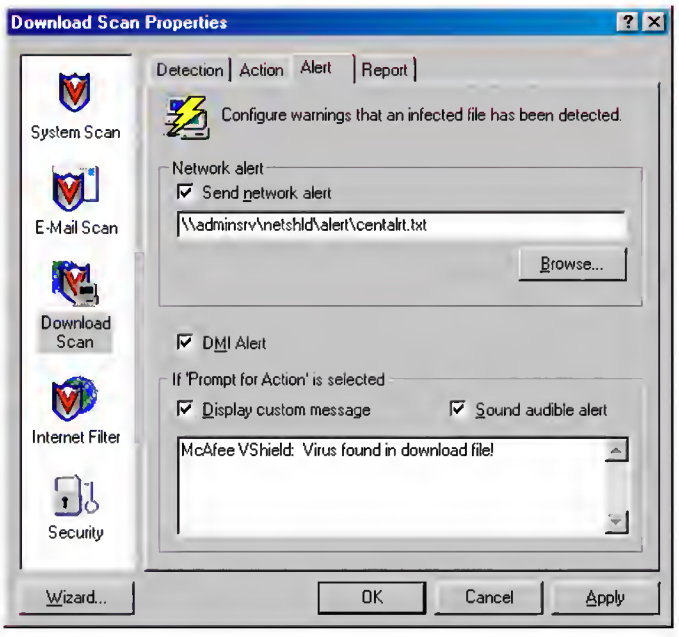

Figure 4-25. Download Scan Properties dialog box - Alert page

2. To tell VShield to send an alert message to a server running NetShield, a Network Associates server-based anti-virus solution, select the **Send network alert** checkbox, then enter the path to the NetShield alert folder on your network, or click **Browse** to locate the correct folder.

NOTE: The folder you choose must contain CENTALRT.TXT, the NetShield Centralized Alerting file. NetShield collects alert messages from VShield and other Network Associates software, then passes them to network administrators for action. To learn more about Centralized Alerting, see the NetShield *User's Guide*.

---

3. To have VShield send virus alert messages via the DMI Component Interface to desktop and network management applications running on your network, select the **DMI Alert** checkbox.

NOTE: The Desktop Management Interface is a standard for communicating management requests and alert information between hardware and software components stored on or connected to desktop computers, and the applications used for managing them. To learn more about using this alert method, consult your network administrator.

---

4. If you chose **Prompt for user action** as your response in the Action page (see "Choosing Action options" on page 112 for details), you can also tell VShield to beep and display a custom message when it finds a virus. To do so, select the **Display custom message** checkbox, then enter the message you want to see in the text box provided—you can enter a message of up to 225 characters in length. Next, select the **Sound audible alert** checkbox.

5. Click the Report tab to choose additional VShield options. To save your changes without closing the Download Scan Properties dialog box, click **Apply**. To save your changes and close the dialog box, click **OK**. To close the dialog box without saving your changes, click **Cancel**.

> **NOTE:** Clicking **Cancel** will not undo any changes you already saved by clicking **Apply**.

Choosing Report options

VShield's Download Scan module lists its current settings and summarizes all of the actions it takes during its scanning operations in a log file called WEBINET.TXT. You can have VShield write its log to this file, or you can use any text editor to create a text file for it to use. You can then open and print the log file for later review from any text editor. Use the Report property page to determine which information VShield will include in its log file.

To set VShield to record its actions in a log file, follow these steps:

1. Click the Report tab in the Download Scan module to display the correct property page (Figure 4-26).

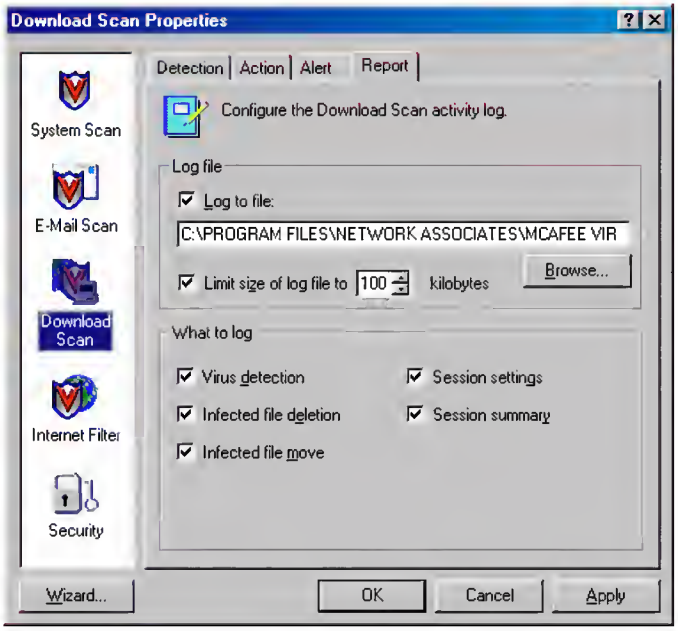

Figure 4-26. Download Scan Properties dialog box - Report page

2. Select the **Log to file** checkbox.

   By default, VShield writes log information to the file WEBINET.TXT in the VirusScan program directory. You can enter a different name and path in the text box provided, or click **Browse** to locate a suitable file elsewhere on your hard disk or on your network.

3. To minimize the log file size, select the **Limit size of log file to** checkbox, then enter a value for the file size, in kilobytes, in the text box provided.

   Enter a value between 10KB and 999KB. By default, VShield limits the file size to 100KB. If the data in the log exceeds the file size you set, VShield erases the existing log and begins again from the point at which it left off.

4. Select the checkboxes that correspond to the information you want VShield to record in its log file. You can choose to record any of this information:

   - **Virus detection.** Select this checkbox to have VShield note the number of infected files it found as you downloaded them.
   - **Infected file deletion.** Select this checkbox to have VShield note the number of infected files it deleted as you downloaded them.

- **Infected file move.** Select this checkbox to have VShield note the number of infected files it moved to your quarantine directory.
- **Session settings.** Select this checkbox to have VShield list the options that you chose in the Download Scan Properties dialog box for each scanning session.
- **Session summary.** Select this checkbox to have VShield summarize its actions during each scanning session. Summary information includes the number of files VShield scanned, the number and type of viruses it detected, the number of files it moved or deleted, and other information.

5. Click a different tab to change any of your Download Scan settings, or click one of the icons along the side of the Download Scan Properties dialog box to choose options for a different module.

   To save your changes in the Download Scan module without closing its dialog box, click **Apply**. To save your changes and close the dialog box, click **OK**. To close the dialog box without saving your changes, click **Cancel**.

   NOTE: Clicking **Cancel** will not undo any changes you already saved by clicking **Apply**.

Configuring the Internet Filter module

Although both Java and ActiveX objects include safeguards designed to prevent harm to your computer system, determined programmers have developed objects that exploit arcane Java or ActiveX features to cause various sorts of harm to your system.

Dangerous objects such as these can often lurk on websites until you visit and download them to your system, usually without realizing that they exist. Most browser software includes a feature that allows you to block Java applets or ActiveX controls altogether, or to turn on security features that authenticate objects before downloading them to your system. But these approaches can deprive you of the interactive benefits of websites you visit by indiscriminately blocking all objects, dangerous or not.

VShield allows a more judicious approach. It uses an up-to-date database of objects known to cause harm to screen Java classes and ActiveX controls you encounter as you browse.

To set VShield to block harmful objects and filter dangerous Internet sites, click the Internet Filter icon at the left side of the VShield Properties dialog box to display the property pages for this module. The next sections describe your options.

Choosing Detection options

VShield starts by blocking all of the harmful objects and sites listed in its database, in order to prevent you from accidentally encountering them (Figure 4-27).

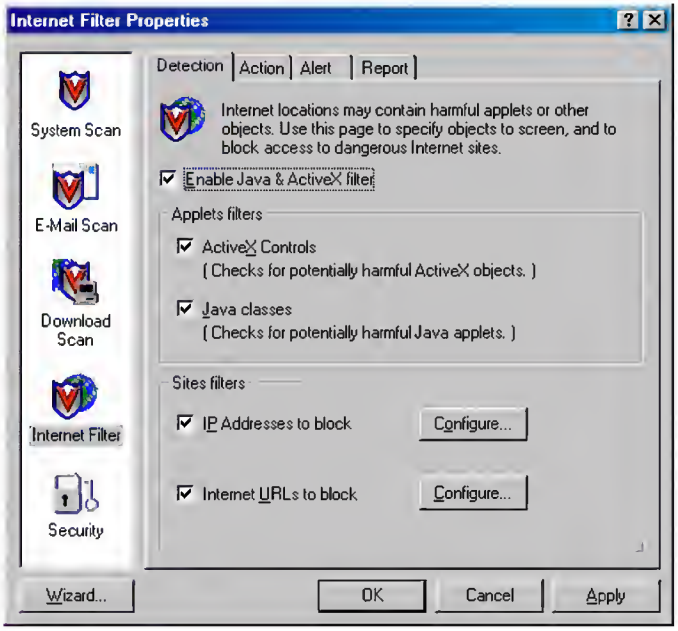

Figure 4-27. Internet Filter Properties - Detection page

To change these default options, verify that the Enable Java & ActiveX filter checkbox is selected, then follow these steps:

1. Tell VShield which objects to filter. Your options are:

   - **ActiveX Controls.** Select this checkbox to have VShield look for and block harmful ActiveX or .OCX controls.
   - **Java classes.** Select this checkbox to have VShield look for and block harmful Java classes, or applets written in Java.

VShield will compare the objects you encounter as you visit Internet sites with an internal database that lists the characteristics of objects known to cause harm. When it finds a match, VShield can alert you and let you decide what to do, or it can automatically keep the object from downloading. See "Choosing Action options" on page 123 more details.

2. Tell VShield which sites to filter. The program uses a list of dangerous Internet sites to decide which ones to prevent your browser from visiting. You can enable this function and add to the list of "banned" sites in two ways:

   - **IP Addresses to block.** Select this checkbox to tell VShield to identify dangerous Internet sites by using their Internet Protocol (IP) addresses. To see or designate which addresses you want VShield to ban, click **Configure** to open the Banned IP Addresses dialog box (Figure 4-28).

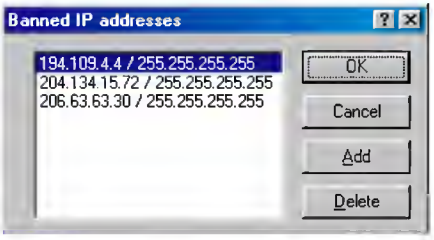

Figure 4-28. Banned IP addresses dialog box

Internet Protocol addresses consist of four groups of three numbers each, formatted in this manner:

123.123.123.123

Each group of numbers can range between zero and 255. VShield can use this number to identify a specific computer or network of computers on the Internet and prevent your browser from connecting to it. In Figure 4-28, each address has two sets of IP numbers. The first is the banned site's domain address—the number you use to find it on the Internet—and the second is a "subnet mask."

A subnet mask is a way to "remap" a range of computer addresses within an internal network. VShield lists a default subnet mask of 255.255.255.255. In most circumstances, you will not need to change this number, but if you know that a particular network node at the site you visit is the source of danger, you might need to enter a subnet mask to preserve your access to other machines at this site.

– To add to the banned list, click **Add**, then type the addresses you want VShield to block in the dialog box that appears (Figure 4-29).

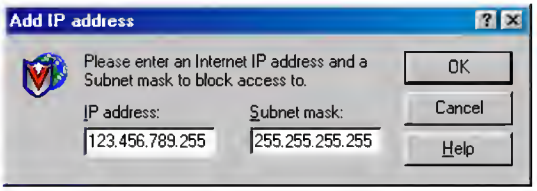

Figure 4-29. Add IP address dialog box

Be sure to enter each address carefully in the correct form. If you know the subnet mask value for the site you want to avoid, enter it in the text box below. Otherwise, leave the default value shown. Click **OK** to save your address and return to the Banned IP Addresses dialog box. To add another address to the list, repeat these steps.

– To remove an address from the banned list, select it, then click **Delete**.

When you have finished editing the list, click **OK** to save your changes and return to the Internet Filter Properties dialog box. Click **Cancel** to close the dialog box without saving your changes.

- **Internet URLs to block.** Select this checkbox to tell VShield to identify dangerous Internet sites by using their Uniform Resource Locator designation. To see or choose which addresses you want VShield to ban, click **Configure** to open the Banned URLs dialog box (Figure 4-30).

Figure 4-30. Banned URLs dialog box

Sometimes used interchangeably with "domain name" or "host name," URLs specify the name and location of a computer on the Internet, usually together with the "transport protocol" you want to use to request a resource from that computer. A complete URL for a website, for instance, would look like:

http://www.dangerdomain.com

The complete URL tells your browser to request the resource via the HyperText Transport Protocol ("http://") from a computer named "www" on a network named "dangerdomain.com." Other transport protocols include "ftp://" and "gopher://." The Internet's Domain Name Server system translates URLs into correct IP addresses using an up-to-date, centralized, and cross-referenced database.

- To add to the banned list, click **Add**, then type the addresses you want VShield to block in the dialog box that appears (Figure 4-31).

Figure 4-31. Add URL dialog box

Be sure to enter each address carefully in the correct form. To ban a website, you can enter *only the domain name*; VShield will assume you mean the HyperText transport protocol. Click **OK** to save your address and return to the Banned IP Addresses dialog box. To add another address to the list, repeat these steps.

- To remove an address from the banned list, select it, then click **Delete**.

When you have finished editing the list, click **OK** to save your changes and return to the Internet Filter Properties dialog box. Click **Cancel** to close the dialog box without saving your changes.

3. Click the Action tab to choose additional VShield options. To save your changes without closing the Internet Filter Properties dialog box, click **Apply**. To save your changes and close the dialog box, click **OK**. To close the dialog box without saving your changes, click **Cancel**.

> **NOTE:** Clicking **Cancel** will not undo any changes you already saved by clicking **Apply**.

Choosing Action options

When VShield encounters a dangerous object or a banned site, it can respond either by asking you whether it should block the object or site, or by automatically blocking it. Use the Action property page to specify which of these courses you want VShield to take.

By default, VShield lets you decide what you want to do (Figure 4-32).

Internet Filter Properties
System Scan
E-Mail Scan
Download Scan
Internet Filter
Security
Detection
Action
Alert
Report
Specify how VShield will respond when it detects a potentially harmful object, or when you attempt to connect to a banned site.
When a potentially harmful object is found
Prompt for user action
You will be prompted to permit or deny access to the dangerous Internet site or to the ActiveX or Java object.
Wizard...
OK
Cancel
Apply

Figure 4-32. Internet Filter Properties dialog box - Action page

Choose a response from the **When a potentially harmful object is found** list. Your choices are:

- **Prompt for user action.** Choose this response to have VShield ask you whether to block a harmful object or site, or to permit access to it.
- **Deny access to objects.** Choose this response to have VShield block harmful objects or sites automatically. The program will do so based on the contents of its own database, plus whatever site information you added. See "Choosing Detection options" on page 119 for details.

Click the Alert tab to choose additional VShield options. To save your changes without closing the Internet Filter Properties dialog box, click **Apply**. To save your changes and close the dialog box, click **OK**. To close the dialog box without saving your changes, click **Cancel**.

NOTE: Clicking **Cancel** will not undo any changes you already saved by clicking **Apply**.

Choosing Alert options

Once you configure it with the response options you want, you can let VShield look for and block harmful objects or Internet sites, with almost no further intervention. If, however, you want VShield to inform you immediately when it encounters such an object or site so you can take appropriate action, you can configure it to send an alert message to you or to others in a variety of ways. Use the Alert property page to choose which alerting methods you want to use.

Follow these steps:

1. Click the Alert tab in the Internet Filter module to display the correct property page (Figure 4-33).

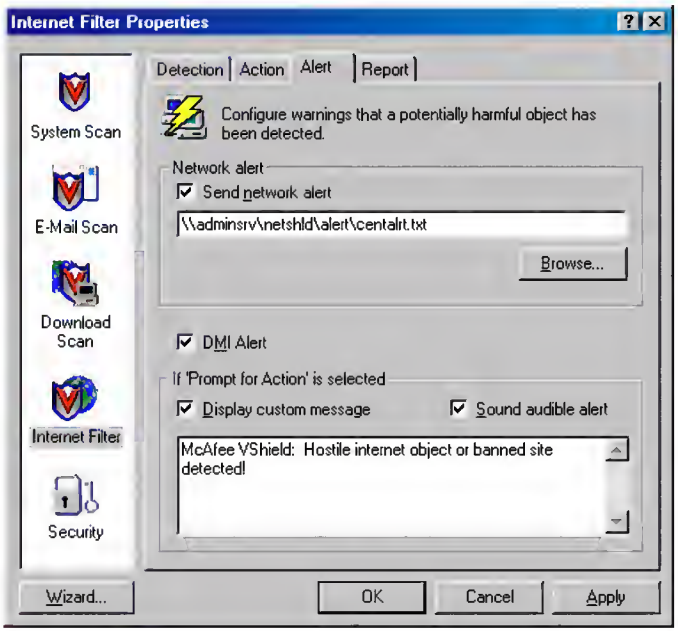

Figure 4-33. Internet Filter Properties dialog box - Alert page

2. To tell VShield to send an alert message to a server running NetShield, a Network Associates server-based anti-virus solution, select the **Send network alert** checkbox, then enter the path to the NetShield alert folder on your network, or click **Browse** to locate the correct folder.

> **NOTE:** The folder you choose must contain CENTALRT.TXT, the NetShield Centralized Alerting file. NetShield collects alert messages from VShield and other Network Associates software, then passes them to network administrators for action. To learn more about Centralized Alerting, see the NetShield *User's Guide*.

3. To have VShield send virus alert messages via the DMI Component Interface to desktop and network management applications running on your network, select the **DMI Alert** checkbox.

> **NOTE:** The Desktop Management Interface is a standard for communicating management requests and alert information between hardware and software components stored on or connected to desktop computers, and the applications used for managing them. To learn more about using this alert method, consult your network administrator.

4. If you chose **Prompt for user action** as your response in the Action page (see "Choosing Action options" on page 123 for details), you can also tell VShield to beep and display a custom message when it finds a virus. To do so, select the **Display custom message** checkbox, then enter the message you want to see in the text box provided—you can enter a message up to 225 characters in length. Next, select the **Sound audible alert** checkbox.

5. Click the Report tab to choose additional VShield options. To save your changes without closing the Internet Filter Properties dialog box, click **Apply**. To save your changes and close the dialog box, click **OK**. To close the dialog box without saving your changes, click **Cancel**.

> **NOTE:** Clicking **Cancel** will not undo any changes you already saved by clicking **Apply**.

Choosing Report options

VShield's Internet Filter module records how many Java and ActiveX objects it scanned, and how many it blocked from access to your computer in a log file called WEBFLTR.TXT. The same file records the number of Internet sites you visited while VShield was active, and how many dangerous sites the program kept your browser from visiting.

You can have VShield write its log to its default file, or you can use any text editor to create a text file for it to use. You can then open and print the log file for later review from any text editor. Use the Report property page to designate the file you want to serve as VShield's Internet Filter log, and to determine that file's permissible size.

To set VShield to record its actions in a log file, follow these steps:

1. Click the Report tab in the Internet Filter module to display the correct property page (Figure 4-34).

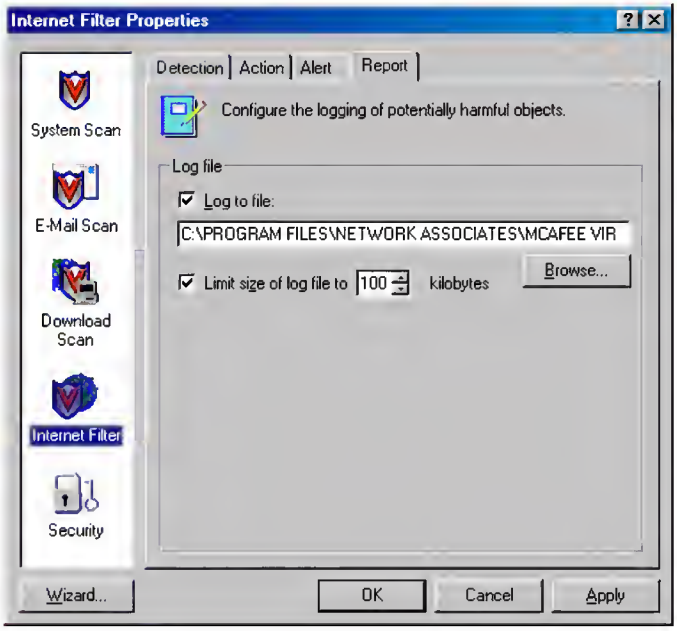

Figure 4-34. Internet Filter Properties dialog box - Report page

2. Select the **Log to file** checkbox.

   By default, VShield writes log information to the file WEBFLTR.TXT in the VirusScan program directory. You can enter a different name and path in the text box provided, or click **Browse** to locate a suitable file elsewhere on your hard disk or on your network.

3. To minimize the log file size, select the **Limit size of log file to** checkbox, then enter a value for the file size, in kilobytes, in the text box provided.

   Enter a value between 10KB and 999KB. By default, VShield limits the file size to 100KB. If the data in the log exceeds the file size you set, VShield erases the existing log and begins again from the point at which it left off.

4. Click a different tab to change any of your Internet Filter settings, or click one of the icons along the side of the Internet Filter Properties dialog box to choose options for a different module.

To save your changes in the Internet Filter module without closing its dialog box, click **Apply**. To save your changes and close the dialog box, click **OK**. To close the dialog box without saving your changes, click **Cancel**.

> **NOTE:** Clicking **Cancel** will not undo any changes you already saved by clicking **Apply**.

Configuring the Security module

To keep the settings you chose for each VShield module safe from unauthorized changes, you can protect any or all module property pages with a password. If you are a system administrator, you can use this feature in conjunction with VShield's ability to save its settings in a .VSH file to replicate your configuration options across all client computers on your network. If you prevent VShield from being disabled (see Step 4 on page 86 for details), then protect that setting with a password, you can enforce a strict anti-virus security policy for all network users, easily and effectively.

Use the Security module to assign a password and to choose which pages to protect.

Enabling password protection

VShield does not enable the Security module by default, because it needs to know which password you want to assign to your settings.

To activate and configure VShield password protection, follow these steps:

1. Select the **Enable password protection** checkbox.

   The options in the rest of the property page activate (Figure 4-35).

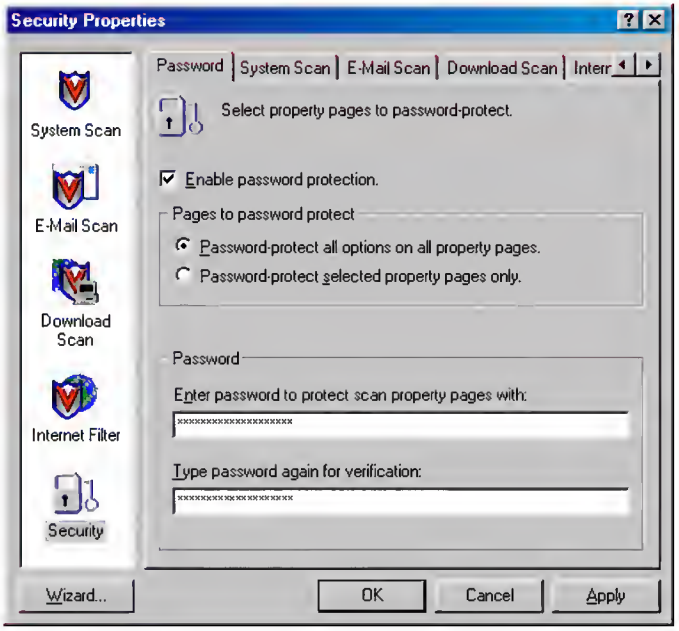

Figure 4-35. Security Properties dialog box - Password page

2. Decide whether to protect the property pages for all VShield modules, or whether to protect individual pages. Your choices are:

   - **Password-protect all options on all property pages.** Select this button to lock everything all at once.
   - **Password-protect selected property pages only.** Select this button to choose which property pages in individual modules you want to lock. The other tabs in the Security Properties dialog box let you designate individual pages.

3. Enter a password to use to lock your settings. Type any combination of up to 20 characters in the upper text box in the **Password** area, then enter the exact same combination in the text box below to confirm your choice.

   IMPORTANT: VShield's password protection is different from the password protection you can assign to VirusScan. Choosing a password for one component does not assign that password to the other component—you must choose passwords for each independently.

4. Click any of the other Security module tabs to protect individual property pages. To save your password without closing the Security Properties dialog box, click **Apply**. If you chose to protect all property pages in all modules and want to close the dialog box, click **OK**. To close the dialog box without saving any changes, click **Cancel**.

   NOTE: Clicking **Cancel** will not undo any changes you already saved by clicking **Apply**.

Once you have protected your settings with a password, VShield will ask you to enter that password whenever you open the VShield Properties dialog box (Figure 4-36).

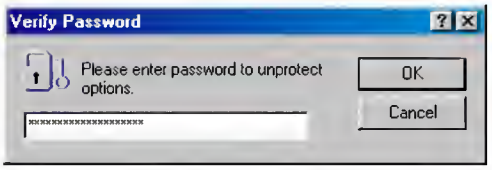

Figure 4-36. Verify Password dialog box

Enter the password you chose in the text box provided, then click **OK** to get access to the VShield Properties dialog box.

Protecting individual property pages

If you chose **Password-protect selected property pages only** in the Security module's Password page, you can choose which configuration options you want to lock.

Follow these steps:

1. Click the tab for the *module* whose settings you want to protect. If you don't see the tab you want, click ◀ or ▶ to bring it into view. A representative page appears in Figure 4-37.

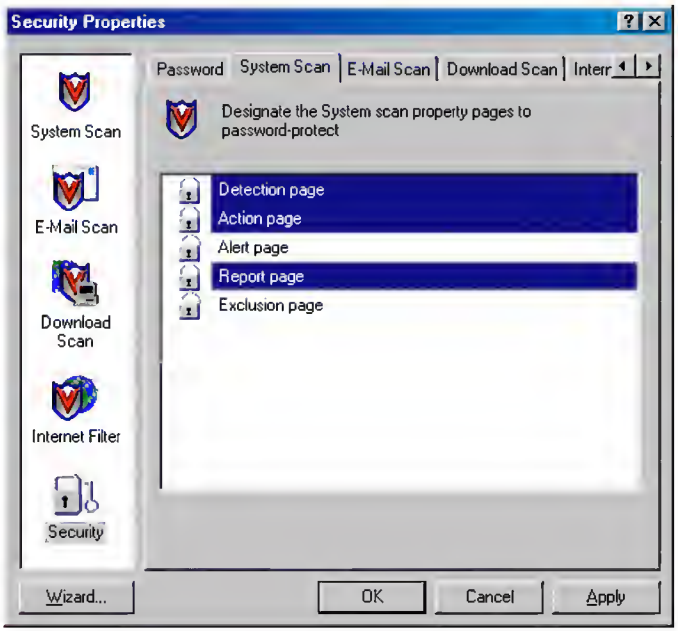

Figure 4-37. System Scan security options

2. Select the settings you want to protect in the list shown.

   You may protect any or all of a module's property pages. Protected property pages display a locked padlock icon in the security list shown in Figure 4-37. To remove protection from a property page, click the locked padlock icon to unlock it.

3. Select as many property pages as you want protected in each module.

4. To save your password without closing the Security Properties dialog box, click **Apply**. To save your changes close the dialog box, click **OK**. To close the dialog box without saving any changes, click **Cancel**.

> **NOTE:** Clicking **Cancel** will not undo any changes you already saved by clicking **Apply**.

Using VShield's shortcut menu

VShield groups several of its common commands in a shortcut menu associated with its system tray icon. Double-click this icon to display the VShield Status dialog box. Click the icon with your right mouse button to display these commands:

- **Status.** Choose this to open the VShield Status dialog box.
- **Properties.** Point to this, then choose one of the VShield modules listed to open the VShield Properties dialog box to the property page for that module.
- **Enable.** Point to this, then choose one of the VShield modules listed to activate or deactivate it. Those modules displayed in the menu with checkmarks are active; those without are inactive.
- **About.** Choose this to display VShield's version number and serial number, the version number and creation date for the current .DAT files in use, and a Network Associates copyright notice.
- **Exit.** Choose this to stop all VShield modules from scanning and to unload VShield from memory.

Disabling or stopping VShield

Once it starts, VShield displays a small icon in the Windows system tray. *Disabling* VShield leaves it running in memory, but keeps it from performing scan functions. When you disable all of its modules, VShield leaves a "cancelled" icon in the Windows system tray that you can use to enable it again.

Stopping VShield removes it from memory entirely—its Windows system tray icon will also disappear. To enable it again at that point, you must open the VShield Properties dialog box and enable each module individually again (see "Setting VShield properties" on page 81 for details) or start it again from VirusScan Scheduler.

You can disable or stop VShield in any of four ways:

- **From the VShield shortcut menu.** Click the VShield icon in the Windows system tray with your right mouse button to display its shortcut menu, then choose **Exit**.

VShield will stop immediately, unload itself from memory and remove its icon from the Windows system tray.

To disable individual VShield modules, right-click the VShield icon, point to **Enable**, then choose each module individually. Those with checkmarks beside them are active; those without checkmarks are disabled.

> **NOTE:** See "Using VShield's shortcut menu" on page 132 to learn more about other menu choices.

- **From the VShield Status dialog box.** Double-click the VShield icon in the Windows system tray to display the VShield Status dialog box (Figure 4-38).

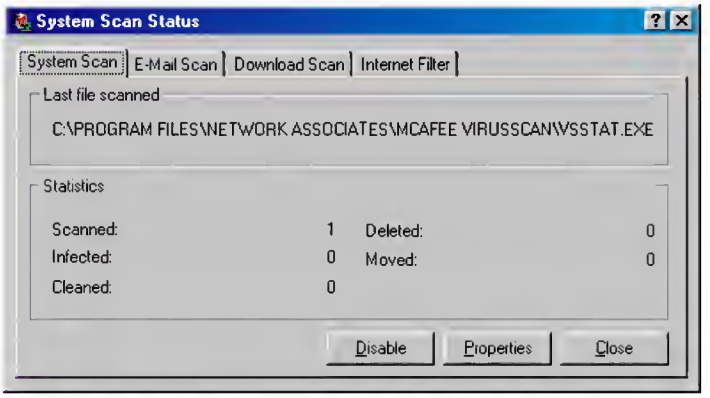

Figure 4-38. VShield Status dialog box

For each module that you want to disable, click the corresponding tab, then click **Disable**. VShield will disable that module immediately. When you have disabled all of its modules, VShield will display in the Windows system tray. To activate each module again, open the Status dialog box, then click **Enable** in each property page.

- **From the VShield Properties dialog box.** Right-click the VShield icon in the Windows system tray, point to **Properties**, then choose **System Scan** from the shortcut menu that appears to display the VShield Properties dialog box (Figure 4-39).

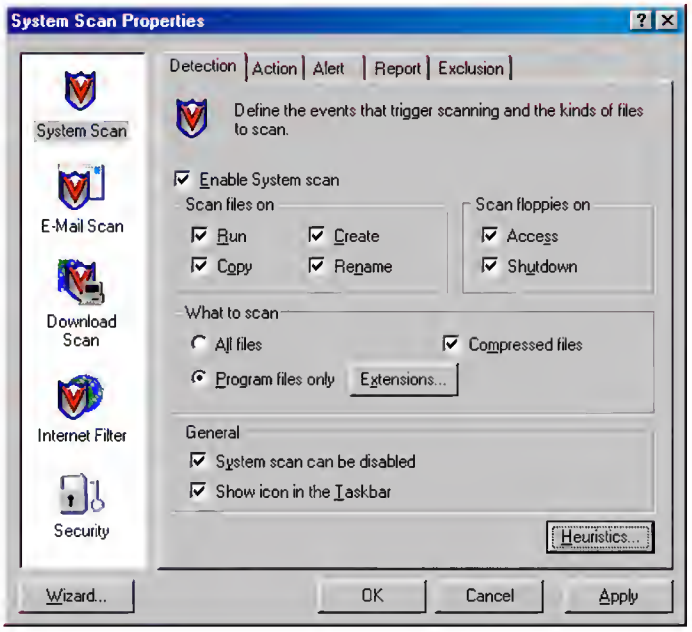

Figure 4-39. VShield Properties dialog box

For each module that you want to disable, click the corresponding icon along the left side of the dialog box, then click the Detection tab. Next, clear the **Enable** checkbox at the top of each page. As you do so, VShield will disable that module. When you have disabled all of its modules, VShield will display in the Windows system tray, unless you have cleared the **Show icon in the taskbar** checkbox.

To activate each module again, open the VShield Properties dialog box, then select the **Enable** checkbox in each module's Detection page.

- **From VirusScan Scheduler.** Click **Start** in the Windows taskbar, point to **Programs**, then to **McAfee VirusScan**. Next, choose **McAfee VirusScan Scheduler** to open the Scheduler window (Figure 4-40).

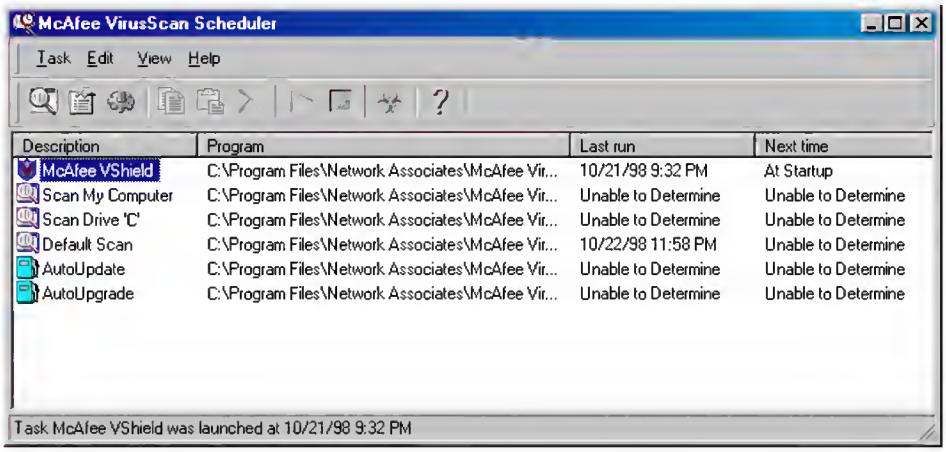

Figure 4-40. VirusScan Scheduler window

Select **McAfee VShield** in the task list, then choose **Disable** from the **Task** menu. VShield will disable all VShield modules and display in the Windows system tray. To start VShield again, select the VShield task, then choose **Enable** from the **Task** menu.

To stop VShield entirely, select **McAfee VShield** in the task list, then click in the Scheduler toolbar. VShield will stop immediately, unload itself from memory and remove its icon from the Windows system tray. To activate it again, select the VShield task, then click .

Tracking VShield status information

Once activated and configured, VShield operates continuously in the background, watching for and then scanning e-mail you receive, files you run or download, or Java and ActiveX objects you encounter.

To see a summary of its progress:

1. Open a VShield Status dialog box. You can do this in two ways:
   - Double-click the VShield system tray icon; to open the Status dialog box shown in Figure 4-38 on page 133; or
   - Open the VirusScan Scheduler, select the VShield task in the task list, then click in the Scheduler toolbar to display the Task Properties dialog box shown in Figure 4-41.

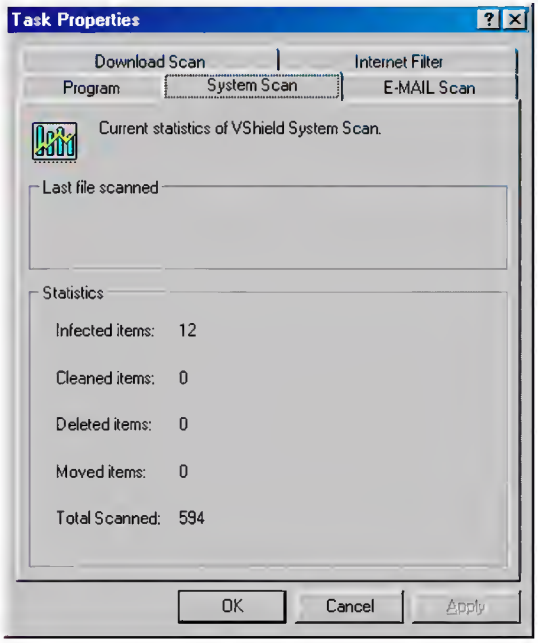

Figure 4-41. VShield Task Properties dialog box

2. Click the tab that corresponds to the program component that you want to enable or disable, or whose progress you want to check.

For the System Scan module, VShield reports the number of files it has scanned, the number of infected files it found, and the number it cleaned, moved or deleted. For the E-mail Scan and Download Scan modules, it reports the number of files it scanned, the number of infections it found, and the number it moved or deleted. For Java and ActiveX applets or Internet sites, VShield reports the number of items it has scanned and the number it has "banned," or kept you from encountering.

If you have activated its reporting feature, VShield also records the same information in the log file for each module.

If you chose the first method described in Step 1 on page 136 to open a Status dialog box, you can also enable or disable VShield, or open the VShield Properties dialog box. You can:

- Click the tab that corresponds to the program component you want to enable or disable, then click **Enable** to start the program component. Click **Disable** to disable it. See "Disabling or stopping VShield" on page 132 to learn more ways to disable and enable VShield.
- Click **Properties** to open the VShield Properties dialog box, where you can set options that tell VShield how to perform each type of scan. See "Setting VShield properties" on page 81 to learn how to choose configuration options in the VShield Properties dialog box.

Using McAfee VirusScan 5

What is VirusScan?

The VirusScan name applies both to the entire set of desktop anti-virus program components described in this *User's Guide*, and to a particular component of that set: SCAN32.EXE, or the VirusScan "on-demand" scanner. "On demand" means that you as a user control when VirusScan starts and ends a scan operation, which targets it examines, what it does when it finds a virus, or any other aspect of the program's operation. Other VirusScan components, by contrast, operate automatically or according to a schedule you set. VirusScan originally consisted solely of an on-demand scanner—features since integrated into the program now provide a cluster of anti-virus functions that give you maximum protection against virus infections and attacks from malicious software.

The VirusScan on-demand component operates in two modes: the VirusScan "Classic" interface gets you up and running quickly, with a minimum of configuration options, but with the full power of the VirusScan anti-virus scanning engine; the VirusScan Advanced mode adds flexibility to the program's configuration options, including the ability to run more than one scan operation concurrently.

This chapter describes how to use VirusScan in both its Classic and Advanced modes.

Why run on-demand scan operations?

Because its VShield component provides background scanning protection, using VirusScan to scan your system might seem redundant. But good anti-virus security measures incorporate complete, regular system scans because:

- **Background scanning checks files as they execute.** VShield looks for virus code as executable files run or when you read a floppy disk, but VirusScan can check for code signatures in files stored on your hard disk. If you rarely run an infected file, VShield might not detect the virus until it deploys its payload. VirusScan, however, can detect a virus as it lies in wait for an opportunity to run.
- **Viruses are sneaky.** Accidentally leaving a floppy disk in your drive as you start your computer could load a virus into memory before VShield loads, particularly if you do not have VShield configured to scan floppy disks. Once in memory, a virus can infect nearly any program, including VShield.

- **Scanning with VShield takes time and resources.** Scanning for viruses as you run, copy or save files can delay, very slightly, software launch times and other tasks. Depending on your situation, this could be time you might rather devote to important work. Although the impact is very slight, you might be tempted to disable VShield if you need every bit of available power for demanding tasks. In that case, performing regular scan operations during idle periods can guard your system against infection without compromising performance.
- **Good security is redundant security.** In the networked, web-centric world in which most computer users operate today, it takes only a moment to download a virus from a source you might not even realize you visited. If a software conflict has disabled background scanning for that moment, or if background scanning is not configured to watch a vulnerable entry point, you could end up with a virus. Regular scan operations can often catch infections before they spread or do any harm.

VirusScan Classic comes with a single, default scan operation pre-configured and ready to run. You can start this scan operation to look for viruses on your C: drive immediately, or you can configure and run your own scan operations to suit your needs. VirusScan Advanced also comes with a single pre-configured scan operation, which scans all of your local hard disks.

Starting VirusScan

To start VirusScan, either

- Click **Start** in the Windows taskbar, point to **Programs**, then to **McAfee VirusScan**. Next, choose **McAfee VirusScan** from the list that appears; or
- Click **Start**, then choose **Run** from the menu that appears. Type SCAN32.EXE in the Run dialog box, then click **OK**.

Both methods open the VirusScan Classic window (Figure 5-1).

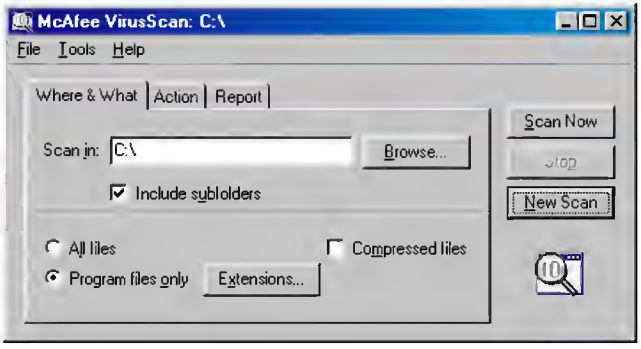

Figure 5-1. VirusScan Classic window

Click **Scan Now** at the right of the window to start the default scan task immediately, or configure a scan task that suits your needs by clicking the tabs at the top of the window and choosing options in each property page.

Using VirusScan menus

The menus along the top of the VirusScan window allow you to change some aspects of the program's operation. You can:

- **Save or restore default settings.** By default, VirusScan Classic will look for viruses in those files most susceptible to virus infection. It will scan your computer's memory and system areas, examine your C: drive and all of its subfolders, then sound an alert and prompt you for a response if it detects a virus. The program will also record its actions and summarize its current settings in a log file that you can review later.

  If you make changes to these settings and want to save your changes so that they become the new default settings, choose **Save As Default** from the **File** menu, or click the **New Scan** button to the right of the VirusScan Classic window. VirusScan will ask you to confirm that you want to replace the file that records the default settings. Click **Overwrite** or **OK** to continue. VirusScan will record your options and use them for every scan operation you run after that.

NOTE: If you make changes to the default settings but decide that you want to return to the settings VirusScan came with originally, use Windows Explorer to locate and delete the file DEFAULT.VSC in the VirusScan program directory. When you next start VirusScan, it will restore its default settings and save them into a new DEFAULT.VSC file. To learn about the .VSC file format, see Appendix C, "Understanding the .VSC File Format."

- **Save new settings.** If you need different VirusScan configurations in order to run various scan operations, or if you want to run a scan operation with the same configuration on more than one computer, you can save your configuration options as a .VSC file with its own name. A .VSC file is a text file that records VirusScan configuration options, much like Windows .INI files record program startup options.

  To save your settings, first configure VirusScan with the options you want, then choose **Save Settings** from the **File** menu. Type a descriptive name in the Save As dialog box, choose a location for the file on your hard disk, then click **Save**. You can then copy this file to any other computer that should also use those settings. See "Configuring VirusScan Classic" on page 143 or "Configuring VirusScan Advanced" on page 149 for more details.

To run VirusScan with these settings, simply locate and double-click the .VSC file you saved. This will start VirusScan with the settings loaded.

- **Open the VirusScan activity log.** Choose **View Activity Log** from the **File** menu to open the log file VirusScan uses to record its actions and settings.

  The log file will open in a Notepad window (Figure 5-2). You can print, edit, copy or otherwise treat this file as you would any ordinary text file. To learn more about what information the log file records, see "Choosing Report options" on page 159.

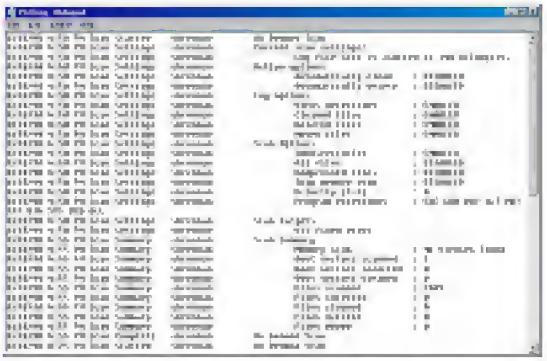

Figure 5-2. VirusScan Activity Log

- **Quit VirusScan.** Choose **Close** from the **File** menu to quit VirusScan. Quitting VirusScan stops any active scan operations, but does *not* affect VShield's continuous background operations. Unless you save them, any configuration options you chose will also disappear when you quit VirusScan.
- **Change VirusScan modes.** Choose **Advanced** from the **Tools** menu to switch from VirusScan Classic to VirusScan Advanced. To switch from VirusScan Advanced to VirusScan Classic, choose **Classic** from the **Tools** menu.
- **Activating password protection.** Choose **Password Protect** from the **Tools** menu to open a dialog box where you can choose which VirusScan configuration options you want to lock in order to prevent unauthorized changes. See "Enabling password protection" on page 163 for details.
- **Start VirusScan Scheduler.** Choose **Scheduler** from the **Tools** menu to open VirusScan Scheduler, a utility that lets you configure and run unattended scan operations. To learn how to use the Scheduler, see "Scheduling Scan Tasks" on page 165.

- **Open the online help file.** Choose **Help Topics** from the **Help** menu to see a list of VirusScan help topics. To see a context-sensitive description of buttons, lists and other items in the VirusScan window, choose **What's this?** from the **Help** menu, then click an item with your left mouse button after your mouse cursor changes to . You can see these same help topics if you right-click an element in the VirusScan window, then choose **What's This?** from the menu that appears.

Configuring VirusScan Classic

To perform a scan operation, VirusScan needs to know what you want it to scan, what you want it to do if it finds a virus, and how it should let you know when it has. You can also tell VirusScan to keep a record of its actions. A series of property pages controls the options for each task—click each tab in the VirusScan Classic window to set up VirusScan for your task.

Choosing Where & What options

VirusScan initially assumes that you want to scan your C: drive and all of its subfolders, and to restrict the files it scans only to those susceptible to virus infection (Figure 5-3).

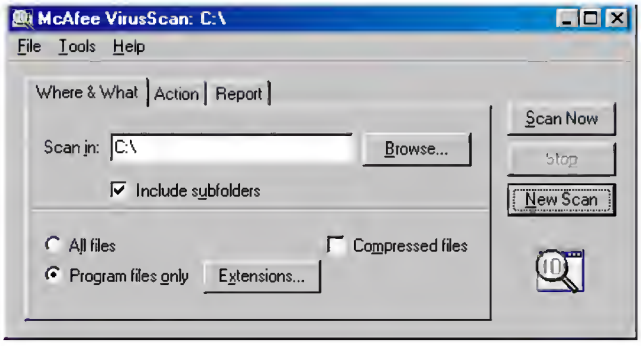

Figure 5-3. VirusScan Classic window - Where & What page

To modify these options, follow these steps:

1. Choose a volume or folder on your system or on your network that you want VirusScan to examine for viruses.

   You can type a path to the target volume or folder in the **Scan in** text box, or click **Browse** to open the Browse for Folder dialog box (Figure 5-4).

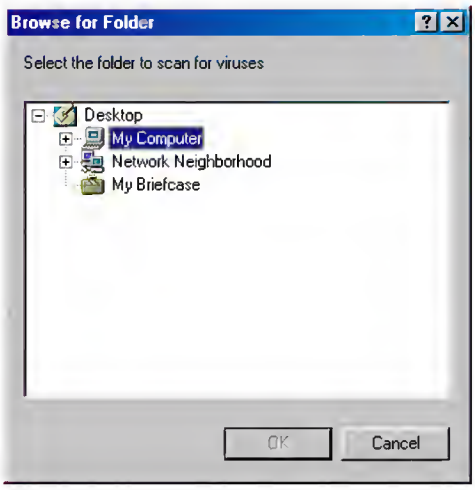

Figure 5-4. Browse for Folder dialog box

Click ⊞ to expand the listing for an item shown in the dialog box. Click ⊟ to collapse an item. You can select hard disks, folders or files as scan targets, whether they reside on your system or on other computers on your network. You cannot select My Computer, Network Neighborhood, or multiple volumes as scan targets from VirusScan Classic—to choose these items as scan targets, you must switch to VirusScan Advanced.

When you have selected your scan target, click **OK** to return to the VirusScan Classic window.

2. Select the **Include subfolders** checkbox to have VirusScan look for viruses in any folders inside your scan target.

3. Specify the types of files you want VirusScan to examine. You can

   - **Scan compressed files.** Select the **Compressed files** checkbox to have VirusScan look for viruses in files compressed with these formats: .??_, .CAB, LZEXE, LZH, PKLite, .TD0, and .ZIP. Although it does give you better protection, scanning compressed files can lengthen a scan operation.

   - **Choose file types for scanning.** Viruses ordinarily cannot infect data files or files that contain no executable code. You can, therefore, safely narrow the scope of your scan operations to those files most susceptible to virus infection in order to speed up scan operations. To do so, select the **Program files only** button. To see or designate the file name extensions VirusScan will examine, click **Extensions** to open the Program File Extensions dialog box (Figure 5-5).

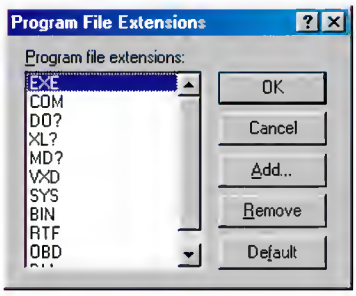

Figure 5-5. Program File Extensions dialog box

By default, VirusScan looks for viruses in files with the extensions .EXE, .COM, .DO?, .XL?, .MD?, .VXD, .SYS, .BIN, .RTF, .OBD, and .DLL. Files with .DO?, .XL?, .RTF, .MD?, and .OBD extensions are Microsoft Office files, all of which can harbor macro virus infections. The ? character is a wildcard that enables VirusScan to scan both document and template files.

- To add to the list, click **Add**, then type the extensions you want VirusScan to scan in the dialog box that appears.
- To remove an extension from the list, select it, then click **Remove**.
- Click **Default** to restore the list to its original form.

When you have finished, click **OK** to close the dialog box.

To have VirusScan examine all files on your system, whatever their extensions, select the **All files** button. This will slow your scan operations down considerably, but will ensure that your system is virus free.

4. Click the Action tab to choose additional VirusScan options.

   To start a scan operation immediately with just the options you've chosen, click **Scan Now**. To save your changes as default scan options, choose **Save As Default** from the **File** menu or click **New Scan**. To save your settings in a new file, choose **Save Settings** from the **File** menu, name your file in the dialog box that appears, then click **Save**.

Choosing Action options

When VirusScan detects a virus, it can respond either by asking you what it should do with the infected file, or by automatically taking an action that you determine ahead of time. Use the Action property page to specify which response options you want VirusScan to give you when it finds a virus, or which actions you want it to take on its own.

Follow these steps:

1. Click the Action tab in the VirusScan Classic window to display the correct property page (Figure 5-6).

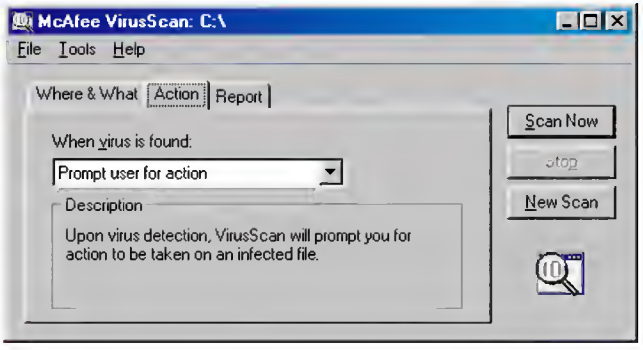

Figure 5-6. VirusScan Classic window - Action page

2. Choose a response from the **When a virus is found** list. The area immediately beneath the list will change to show you additional options for each response. Your choices are:

   - **Prompt User for Action.** Choose this response if you expect to be at your computer when VirusScan scans your disk—VirusScan will display an alert message when it finds a virus and offer you the full range of its available response options.
   - **Move infected files automatically**. Choose this response to have VirusScan move infected files to a quarantine directory as soon as it finds them. By default, VirusScan moves these files to a folder named INFECTED that it creates at the root level of the drive on which it found the virus. For example, if VirusScan found an infected file in T:\MY DOCUMENTS and you specified INFECTED as the quarantine directory, VirusScan would copy the file to T:\INFECTED.

     You can enter a different name in the text box provided, or click **Browse** to locate a suitable folder on your hard disk.
   - **Clean infected files automatically.** Choose this response to tell VirusScan to remove the virus code from the infected file as soon as it finds it. If VirusScan cannot remove the virus, it will note the incident in its log file. See "Choosing Report options" on page 159 for details.
   - **Delete infected files automatically.** Use this option to have VirusScan delete every infected file it finds immediately. Be sure to enable its reporting feature so that you have a record of which files VirusScan deleted. You will need to restore deleted files from backup copies. If VirusScan cannot delete an infected file, it will note the incident in its log file.
   - **Continue scanning.** Use this option only if you plan to leave your computer unattended while VirusScan checks for viruses. If you also activate the VirusScan reporting feature (see "Choosing Report options" on page 159 for details), the program will record the names of any viruses it finds and the names of infected files so that you can delete them at your next opportunity.

3. Click the Report tab to choose additional VirusScan options.

   To start a scan operation immediately with just the options you've chosen, click **Scan Now**. To save your changes as default scan options, choose **Save As Default** from the **File** menu or click **New Scan**. To save your settings in a new file, choose **Save Settings** from the **File** menu, name your file in the dialog box that appears, then click **Save**.

Choosing Report options

By default, VirusScan beeps to alert you when it finds a virus. You can use the Report page to enable or disable this alert, or to add an alert message to the Virus Found dialog box that appears when VirusScan finds an infected file. This alert message can contain any information, from a simple warning to instructions about how to report the incident to a network administrator.

This same page determines the size and location of VirusScan's log file. By default, the program lists its current settings and summarizes all of the actions it takes during its scanning operations in a log file called VSCLOG.TXT. You can have VirusScan write its log to this file, or you can use any text editor to create a text file for VirusScan to use. You can then open and print the log file for later review from within VirusScan or from your text editor.

To choose VirusScan alert and log options, follow these steps:

1. Click the Report tab in the VirusScan Classic window to display the correct property page (Figure 5-7).

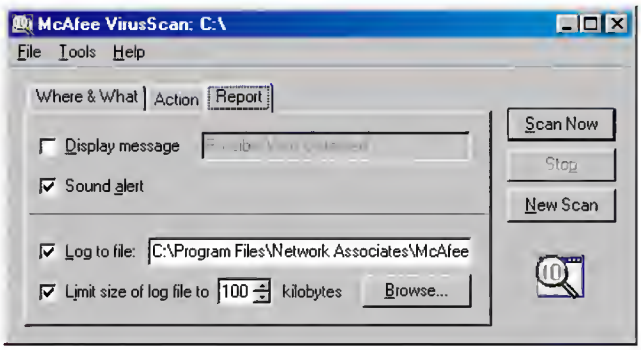

Figure 5-7. VirusScan Classic window - Report page

2. Choose the types of alert methods you want VirusScan to use when it finds a virus. You can have VirusScan:

   - **Display a custom message.** Select the **Display message** checkbox, then enter the message you want to appear in the text box provided. You can enter a message up to 225 characters in length.

     NOTE: To have VirusScan display your message, you must have selected **Prompt user for action** as your response in the Action page (see "Choosing Action options" on page 154 for details).

- **Beep.** Select the **Sound alert** checkbox.

3. Select the **Log to file** checkbox.

   By default, VirusScan writes log information to the file VSCLOG.TXT in the VirusScan program directory. You can enter a different name and path in the text box provided, or click **Browse** to locate a suitable file elsewhere on your hard disk or on your network.

4. To minimize the log file size, select the **Limit size of log file to** checkbox, then enter a value for the file size, in kilobytes, in the text box provided.

   Enter a value between 10KB and 999KB. By default, VirusScan limits the file size to 100KB. If the data in the log exceeds the file size you set, VirusScan erases the existing log and begins again from the point at which it left off.

5. Click a different tab to change any of your VirusScan settings.

   To start a scan operation immediately with the options you've chosen, click **Scan Now**. To save your changes as default scan options, choose **Save As Default** from the **File** menu or click **New Scan**. To save your settings in a new file, choose **Save Settings** from the **File** menu, name your file in the dialog box that appears, then click **Save**.

Configuring VirusScan Advanced

VirusScan Advanced offers you more flexibility in your configuration options than does VirusScan Classic, including the ability to run more than one scan operation concurrently, the ability to exclude items from scan operations, and the ability to activate VirusScan's heuristic detection capability.

Starting VirusScan Advanced

To start VirusScan Advanced, follow these steps:

1. Click **Start** in the Windows taskbar, point to **Programs**, then to **McAfee VirusScan**. Next, choose **McAfee VirusScan** from the list that appears.

   This opens the VirusScan Classic window (see Figure 5-1 on page 140).

2. Choose **Advanced** from the **Tools** menu in the VirusScan Classic window to switch to VirusScan Advanced mode.

As with VirusScan Classic a series of property pages controls the options for each task in VirusScan Advanced. Click each tab in the VirusScan Advanced window to set up VirusScan for your task. The next sections describe the options you have available.

Choosing Detection options

VirusScan initially assumes that you want to scan all hard disks on your computer, including those mapped from network drives, and to restrict the files it scans only to those susceptible to virus infection (Figure 5-8).

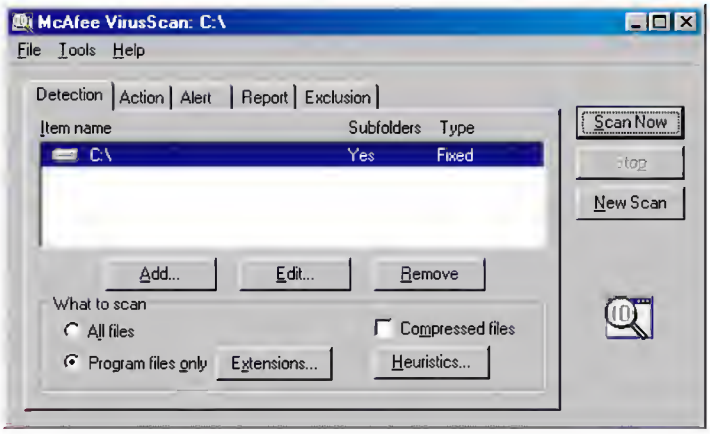

Figure 5-8. VirusScan Advanced window - Detection page

To modify these options and add others, follow these steps:

1. Choose which parts of your system or your network that you want VirusScan to examine for viruses. You can:

   - **Add scan targets.** Click **Add** to open the Add Scan Item dialog box (Figure 5-9).

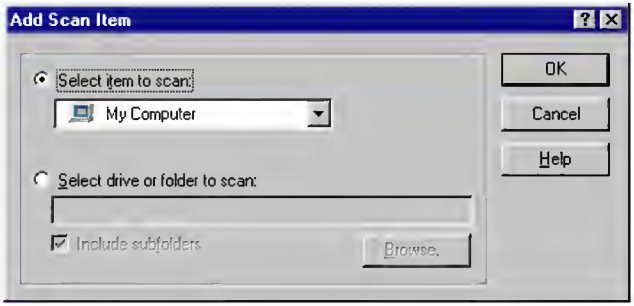

Figure 5-9. Add Scan Item dialog box

To have VirusScan examine your entire computer or a subset of the drives on your system or your network, click the **Select item to scan** button, then choose the scan target from the list provided.

Your choices are:

- **My Computer.** This tells VirusScan to scan all drives physically attached to your computer or logically mapped via Windows Explorer to a drive letter on your computer.
- **All Removable Media.** This tells VirusScan to scan only CD-ROM discs, Iomega ZIP disks, or similar storage devices physically attached to your computer.
- **All Fixed Disks.** This tells VirusScan to scan hard disks physically connected to your computer.
- **All Network Drives.** This tells VirusScan to scan all drives logically mapped via Windows Explorer to a drive letter on your computer.

To have VirusScan examine a particular disk or folder on your system, click the **Select drive or folder to scan** button. Next, type in the text box provided the drive letter or the path to the folder you want scanned, or click **Browse** to locate the scan target on your computer. Select the **Include subfolders** checkbox to have VirusScan also look for viruses in any folders inside your scan target. Click **OK** to close the dialog box.

- **Change scan targets.** Select one of the listed scan targets, then click **Edit** to open the Edit Item to Scan dialog box (Figure 5-10).

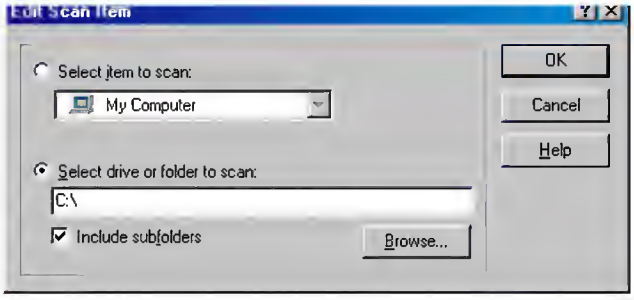

Figure 5-10. Edit Scan Item dialog box

The dialog box appears with the existing scan target specified. Choose or enter a new scan target, then click **OK** to close the dialog box.

- **Remove scan targets.** Select one of the listed scan targets, then click **Remove** to delete it.

2. Specify the types of files you want VirusScan to examine. You can

   - **Scan compressed files.** Select the **Compressed files** checkbox to have VirusScan look for viruses in files compressed with these formats: .??_, .CAB, LZEXE, LZH, PKLite, .TD0, and .ZIP. Although it does give you better protection, scanning compressed files can increase the time that a scan operation takes.

   - **Choose file types for scanning.** Viruses ordinarily cannot infect data files or files that contain no executable code. You can, therefore, safely narrow the scope of your scan operations to those files most susceptible to virus infection in order to speed up scan operations. To do so, select the **Program files only** button. To see or designate the file name extensions VirusScan will examine, click **Extensions** to open the Program File Extensions dialog box (Figure 5-11).

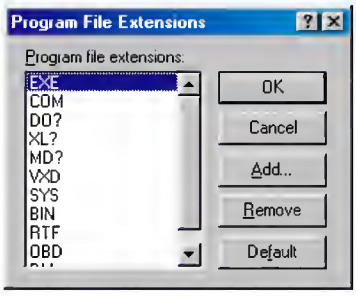

Figure 5-11. Program File Extensions dialog box

By default, VirusScan looks for viruses in files with the extensions .EXE, .COM, .DO?, .XL?, .MD?, .VXD, .SYS, .BIN, .RTF, .OBD, and .DLL. Files with .DO?, .XL?, .MD?, .RTF, and .OBD extensions are Microsoft Office files, all of which can harbor macro virus infections. The ? character is a wildcard that enables VirusScan to scan both document and template files.

   - To add to the list, click **Add**, then type the extensions you want VirusScan to scan in the dialog box that appears.

   - To remove an extension from the list, select it, then click **Remove**.

   - Click **Default** to restore the list to its original form.

   When you have finished, click **OK** to close the dialog box.

   To have VirusScan examine all files on your system, whatever their extensions, select the **All files** button. This will slow your scan operations down considerably, but will ensure that your system is virus free.

- **Turn on heuristic scanning**. Click **Heuristics** to open the Heuristics Scan Settings dialog box (Figure 5-12).

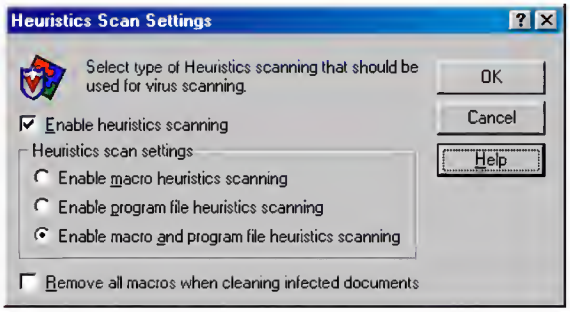
Heuristics Scan Settings
Select type of Heuristics scanning that should be used for virus scanning.
OK
Cancel
Help
Enable heuristics scanning
Heuristics scan settings
Enable macro heuristics scanning
Enable program file heuristics scanning
Enable macro and program file heuristics scanning
Remove all macros when cleaning infected documents

Figure 5-12. Heuristics Scan Settings dialog box

Heuristic scan technology enables VirusScan to recognize new viruses based on their resemblance to similar viruses VirusScan already knows. To do this, the program looks for "virus-like" characteristics in the files you've asked it to scan. The presence of a sufficient number of these characteristics in a file leads VirusScan to identify the file as potentially infected with a new or previously unidentified virus.

Because VirusScan looks simultaneously for file characteristics that rule out the possibility of virus infection, it will rarely give you a false indication of a virus infection. Therefore, unless you know that the file does *not* contain a virus, you should treat "potential" infections with the same caution you would confirmed infections.

To activate heuristic scanning, follow these steps:

a. Select the **Enable heuristics scanning** checkbox. The remaining options in the dialog box activate.

b. Select the types of heuristic scanning you want VirusScan to use. Your choices are:

   - **Enable macro heuristics scanning**. Choose this option to have VirusScan identify all Microsoft Word, Microsoft Excel, and other Microsoft Office files that have embedded macros, then compare the macro code to its virus signature database. VirusScan will identify exact matches with the virus name; code signatures that resemble existing viruses cause VirusScan to tell you it has found a potential macro virus.

- **Enable program file heuristics scanning.** Choose this option to have VirusScan locate new viruses in program files by examining their characteristics and comparing them against a list of known virus characteristics. VirusScan will identify files with a sufficient number of these characteristics as potential viruses.
- **Enable macro and program file heuristics scanning.** Choose this option to have VirusScan use both types of heuristic scanning. Network Associates recommends that you use this option for complete anti-virus protection.

c. Determine how you want to treat infected macro files. Select **Remove all macros when cleaning infected documents** to eliminate all infectable code from the document and leave only data. To try to remove only the virus code from the document's macros, leave this checkbox clear.

> **WARNING:** Use this feature with caution: removing all macros from a document can cause it to lose data or to become corrupted and unusable.

d. Click **OK** to save your settings and return to the VirusScan Advanced window.

3. Click the Action tab to choose additional VirusScan options.

   To start a scan operation immediately with just the options you've chosen, click **Scan Now**. To save your changes as default scan options, choose **Save As Default** from the **File** menu or click **New Scan**. To save your settings in a new file, choose **Save Settings** from the **File** menu, name your file in the dialog box that appears, then click **Save**.

Choosing Action options

When VirusScan detects a virus, it can respond either by asking you what it should do with the infected file, or by automatically taking an action that you determine ahead of time. Use the Action property page to specify which response options you want VirusScan to give you when it finds a virus, or which actions you want it to take on its own.

Follow these steps:

1. Click the Action tab in the VirusScan Advanced window to display the correct property page (Figure 5-13).

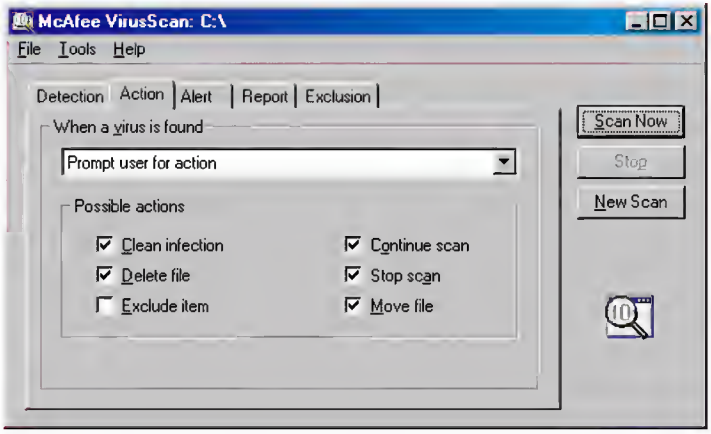

Figure 5-13. VirusScan Advanced - Action page

2. Choose a response from the **When a virus is found** list. The area immediately beneath the list will change to show you additional options for each response. Your choices are:

   - **Prompt User for Action.** Choose this response if you expect to be at your computer when VirusScan examines your disk—the program will display an alert message when it finds a virus and offer you a range of possible responses. Select the response options you want to see in the alert message:
     - **Clean infection.** This option tells VirusScan to try to remove the virus code from the infected file.
     - **Delete file.** This option tells VirusScan to delete the infected file immediately.
     - **Exclude item.** This option tells VirusScan to skip the file during later scan operations. This is the only option not selected by default.
     - **Continue scan.** This option tells VirusScan to continue with its scan, but not take any other actions. If you have its reporting options enabled, VirusScan records the incident in its log file.
     - **Stop scan.** This option tells VirusScan to stop the scan operation immediately. To continue, you must click **Scan Now** to restart the operation.
     - **Move file.** This option tells VirusScan to move the infected file to a quarantine folder.

- **Move infected files automatically**. Choose this response to have VirusScan move infected files to a quarantine directory as soon as it finds them. By default, VirusScan moves these files to a folder named INFECTED that it creates at the root level of the drive on which it found the virus. For example, if VirusScan found an infected file in T:\MY DOCUMENTS and you specified INFECTED as the quarantine directory, VirusScan would copy the file to T:\INFECTED.

  You can enter a different name in the text box provided, or click **Browse** to locate a suitable folder on your hard disk.

- **Clean infected files automatically.** Choose this response to have VirusScan remove the virus code from the infected file as soon as it finds it. If VirusScan cannot remove the virus, it will note the incident in its log file if you have its reporting feature enabled. See "Choosing Report options" on page 159 for details.

- **Delete infected files automatically.** Choose this response to have VirusScan delete every infected file it finds immediately. Be sure to enable its reporting feature so that you have a record of which files VirusScan deleted. You will need to restore deleted files from backup copies.

- **Continue scanning.** Choose this response only if you plan to leave your computer unattended while VirusScan checks for viruses. If you also activate the VirusScan reporting feature (see "Choosing Report options" on page 159 for details), the program will record the names of any viruses it finds and the names of infected files so that you can delete them at your next opportunity.

3. Click the Alert tab to choose additional VirusScan configuration options.

   To start a scan operation immediately with just the options you've chosen, click **Scan Now**. To save your changes as default scan options, choose **Save As Default** from the **File** menu or click **New Scan**. To save your settings in a new file, choose **Save Settings** from the **File** menu, name your file in the dialog box that appears, then click **Save**.

Choosing Alert options

Once you configure it with the response options you want, you can let VirusScan look for and remove viruses from your system automatically, as it finds them, with almost no further intervention. If, however, you want VirusScan to inform you immediately when it finds a virus so that you can take appropriate action, you can configure it to send an alert message to you in a variety of ways. Use the Alert property page to choose which alerting methods you want to use.

Follow these steps:

1. Click the Alert tab in the VirusScan Advanced window to display the correct property page (Figure 5-14).

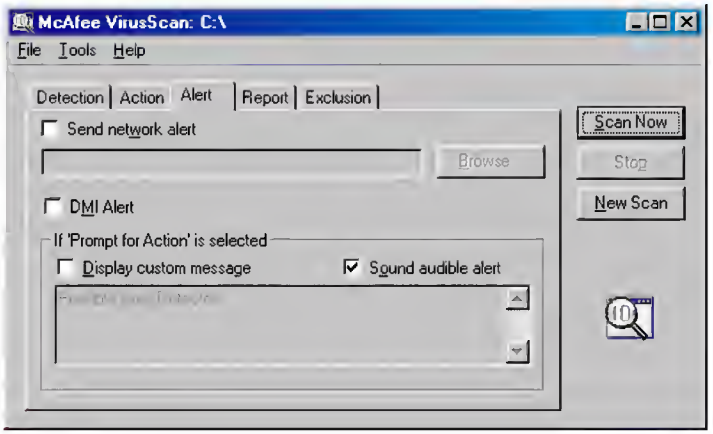

Figure 5-14. VirusScan Advanced - Alert page

2. To tell VirusScan to send an alert message to a server running NetShield, a Network Associates server-based anti-virus solution, select the **Send network alert** checkbox, then enter the path to the NetShield alert folder on your network, or click **Browse** to locate the correct folder.

> **NOTE:** The folder you choose must contain CENTALRT.TXT, the NetShield Centralized Alerting file. NetShield collects alert messages from VirusScan and other Network Associates software, then passes them to network administrators for action. To learn more about Centralized Alerting, see the NetShield *User's Guide*.

3. To have VirusScan send virus alert messages via the DMI Component Interface to desktop and network management applications running on your network, select the **DMI Alert** checkbox.

> **NOTE:** The Desktop Management Interface is a standard for communicating management requests and alert information between hardware and software components stored on or connected to desktop computers, and the applications used for managing them. To learn more about using this alert method, see your network administrator.

4. If you chose **Prompt user for action** as your response in the Action page (see "Choosing Action options" on page 154 for details), you can also tell VirusScan to beep and display a custom message when it finds a virus. To do so, select the **Display custom message** checkbox, then enter the message you want to see in the text box provided—you can enter a message up to 225 characters in length. Next, select the **Sound audible alert** checkbox.

5. Click the Report tab to choose additional VirusScan configuration options.

   To start a scan operation immediately with just the options you've chosen, click **Scan Now**. To save your changes as default scan options, choose **Save As Default** from the **File** menu or click **New Scan**. To save your settings in a new file, choose **Save Settings** from the **File** menu, name your file in the dialog box that appears, then click **Save**.

Choosing Report options

VirusScan lists its current settings and summarizes all of the actions it takes during its scanning operations in a log file called VSCLOG.TXT. You can have VirusScan write its log to this file, or you can use any text editor to create a text file for VirusScan to use. You can then open and print the log file for later review from within VirusScan or from your text editor.

The VSCLOG.TXT file can serve as an important management tool for you to track virus activity on your system and to note which settings you used to detect and respond to the infections VirusScan found. You can also use the incident reports recorded in the file to determine which files you need to replace from backup copies, examine in quarantine, or delete from your computer. Use the Reports property page to determine which information VirusScan will include in its log file.

To set VirusScan to record its actions in a log file, follow these steps:

1. Click the Report tab in the VirusScan Advanced window to display the correct property page (Figure 5-15).

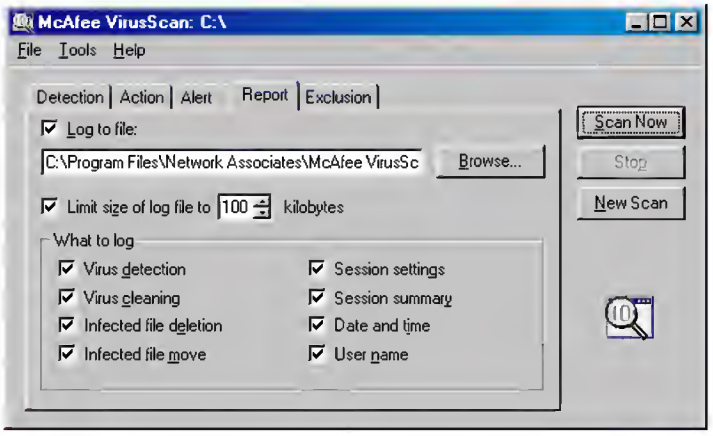

Figure 5-15. VirusScan Advanced - Report page

2. Select the **Log to file** checkbox.

   By default, VirusScan writes log information to the file VSCLOG.TXT in the VirusScan program directory. You can enter a different name in the text box provided, or click **Browse** to locate a suitable file elsewhere on your hard disk or on your network.

3. To minimize the log file size, select the **Limit size of log file to** checkbox, then enter a value for the file size, in kilobytes, in the text box provided.

Enter a value between 10KB and 999KB. By default, VirusScan limits the file size to 100KB. If the data in the log exceeds the file size you set, VirusScan erases the existing log and begins again from the point at which it left off.

4. Select the checkboxes that correspond to the information you want VirusScan to record in its log file. You can choose to record any of this information:

   - **Virus detection.** Select this checkbox to have VirusScan note the number of infected files it found during this scanning session.
   - **Virus cleaning.** Select this checkbox to have VirusScan note the number of infected files from which it removed the infecting virus.
   - **Infected file deletion.** Select this checkbox to have VirusScan note the number of infected files it deleted from your system.
   - **Infected file move.** Select this checkbox to have VirusScan note the number of infected files it moved to your quarantine directory.
   - **Session settings.** Select this checkbox to have VirusScan list the options you choose in the McAfee VirusScan Properties dialog box for each scanning session.
   - **Session summary.** Select this checkbox to have VirusScan summarize its actions during each scanning session. Summary information includes the number of files scanned, the number and type of viruses detected, the number of files moved or deleted, and other information.
   - **Date and time.** Select this checkbox to have VirusScan append the date and time to each log entry it records.
   - **User name.** Select this checkbox to have VirusScan append the name of the user logged in to your computer at the time it records each log entry.

   To see the contents of the log file, start VirusScan, then choose **View Activity Log** from the **File** menu. For more information, see "Using VirusScan menus" on page 141.

5. Click the Exclusion tab to choose additional VirusScan configuration options.

   To start a scan operation immediately with just the options you've chosen, click **Scan Now**. To save your changes as default scan options, choose **Save As Default** from the **File** menu or click **New Scan**. To save your settings in a new file, choose **Save Settings** from the **File** menu, name your file in the dialog box that appears, then click **Save**.

Choosing Exclusion options

Many of the files stored on your computer are not vulnerable to virus infection. Scan operations that examine these files can take a long time and produce few results. You can speed up scan operations by telling VirusScan to look only at susceptible file types (see "Choosing Detection options" on page 150 for details), or you can tell VirusScan to ignore entire files or folders that you know cannot become infected.

Once you scan your system thoroughly, you can exclude the files and folders that do not change or that are not normally vulnerable to virus infection. You can also rely on VShield to provide you with protection between scheduled scan operations. Regular scan operations that examine all areas of your computer, however, provide you with the best virus defense.

To exclude files or folders from scan operations, follow these steps:

1. Click the Exclusion tab in the VirusScan Advanced window to display the correct property page (Figure 5-16).

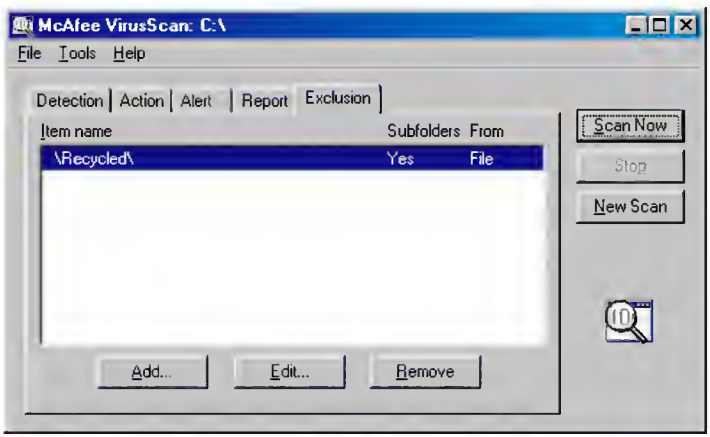

Figure 5-16. VirusScan Advanced window - Exclusion page

The Exclusion page will initially list only your Recycle Bin. VirusScan excludes the Recycle Bin from scan operations because Windows will not run files stored there.

2. Specify the items you want to exclude. You can
   - **Add files, folders or volumes to the exclusion list.** Click **Add** to open the Add Exclude Item dialog box (Figure 5-17).

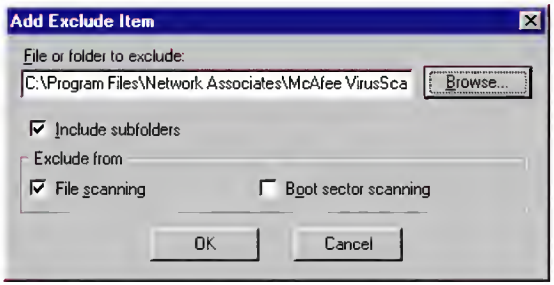

Figure 5-17. Add Exclude Item dialog box

a. Type the volume, the path to the file, or the path to the folder that you want to exclude from scanning, or click **Browse** to locate a file or folder on your computer.

> **NOTE:** If you have chosen to move infected files to a quarantine folder automatically, the program excludes that folder from scan operations.

b. Select the **Include Subfolders** checkbox to exclude all subfolders within the folder you just specified.

c. Select the **File scanning** checkbox to tell VirusScan not to look for file-infector viruses in the files or folders you exclude.

d. Select the **Boot sector scanning** checkbox to tell VirusScan not to look for boot-sector viruses in the files or folders you exclude. Use this option to exclude system files, such as COMMAND.COM, from scan operations.

> **WARNING:** Network Associates recommends that you do *not* exclude your system files from virus scanning.

e. Click **OK** to save your changes and close the dialog box.

f. Repeat steps a. through d. until you have listed all of the files and folders you do not want scanned.

- **Change the exclusion list.** To change the settings for an exclusion item, select it in the Exclusions list, then click **Edit** to open the Edit Exclude Item dialog box. Make the changes you need, then click **OK** to close the dialog box.

- **Remove an item from the list.** To delete an exclusion item, select it in the list, then click **Remove**. VirusScan will then scan this file or folder during its next scanning operation.

3. Click a different tab to change any of your VirusScan configuration settings.

   To start a scan operation immediately with the options you've chosen, click **Scan Now**. To save your changes as default scan options, choose **Save As Default** from the **File** menu or click **New Scan**. To save your settings in a new file, choose **Save Settings** from the **File** menu, name your file in the dialog box that appears, then click **Save**.

Enabling password protection

VirusScan lets you set a password to protect the settings you choose in each property page from unauthorized changes. This feature is particularly useful for system administrators who need to keep users from tampering with their security measures by changing VirusScan settings. Use the Security property page to lock your settings.

To enable password protection for VirusScan Advanced, follow these steps:

1. Choose **Password Protect** from the **Tools** menu in the VirusScan Advanced window to open the Password Protection dialog box (Figure 5-18).

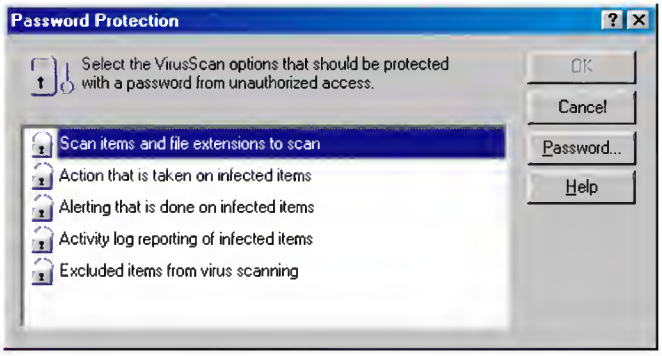
Password Protection
Select the VirusScan options that should be protected with a password from unauthorized access.
OK
Cancel
Password...
Help
Scan items and file extensions to scan
Action that is taken on infected items
Alerting that is done on infected items
Activity log reporting of infected items
Excluded items from virus scanning

Figure 5-18. Password Protection dialog box

2. Select the settings you want to protect in the list shown.

   You may protect any or all VirusScan property pages. Protected property pages display a locked padlock icon in the security list shown in Figure 5-18. To remove protection from a property page, click the locked padlock icon to unlock it.

3. Click **Password** to open the Specify Password dialog box (Figure 5-19).

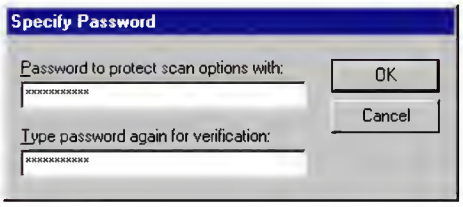

Figure 5-19. Specify Password dialog box

   a. Enter a password in the first text box shown, then enter the same password again in the text box below to confirm your choice.

   b. Click **OK** to close the Specify Password dialog box.

4. Click **OK** to return to the VirusScan Advanced window.

Scheduling Scan Tasks 6

What does VirusScan Scheduler do?

VirusScan Scheduler runs scan operations and other tasks on the dates and at the times you choose, or at intervals you set. Use the Scheduler to run a scan operation in your absence, when it causes the least disruption to your work, as part of a series of automated tasks, or in other ways that suit your needs.

Why schedule scan operations?

Although VirusScan includes components that look for viruses continuously or that allow you to scan your system whenever you want, you can schedule regular scan operations and other VirusScan activities to

- **Set a periodic baseline for your system.** If you want to track your system or your network for recurring virus activity, schedule a full scan of your system at regular intervals. VirusScan's reporting features can provide you with a complete report on the number, type, size and other characteristics of any viruses it finds.
- **Supplement or replace on-access scanning.** Network Associates recommends that you use VShield to scan continuously for viruses, but if your environment doesn't permit you to use VShield or if you have other concerns about system performance, schedule frequent scan operations to prevent infections. Even if you do use VShield, scheduling periodic full scans of your system reduces the likelihood that infected files remain undetected.
- **Alternate between scan operations.** Scheduled scanning operations give you the flexibility to choose different operations for different purposes or different times. If, for example, you want to use VShield to scan your own system continuously and scan mapped network drives less frequently, you can schedule a task for this purpose.

The Scheduler comes with a default set of tasks already configured, but not yet scheduled. This set includes tasks that start VShield when you start your computer, that perform a default scan task, that scan your C: drive, that scan all drives on your system, and that update VirusScan's data files and program components. You can enable one of the default tasks to start, or you can create your own tasks to suit your work habits.

Starting the VirusScan Scheduler

To start the VirusScan Scheduler, either

- Click **Start**, point to **Programs**, then to **McAfee VirusScan**. Next, choose **McAfee VirusScan Scheduler** from the list that appears; or
- Start VirusScan Classic, then choose **Scheduler** from the **Tools** menu. To learn how to start VirusScan, see Chapter 5, "Using McAfee VirusScan."

Both methods open the Scheduler window (Figure 6-1). Once you start it, the Scheduler also displays a small icon in the Windows system tray. Double-click this icon to bring the Scheduler window to the foreground.

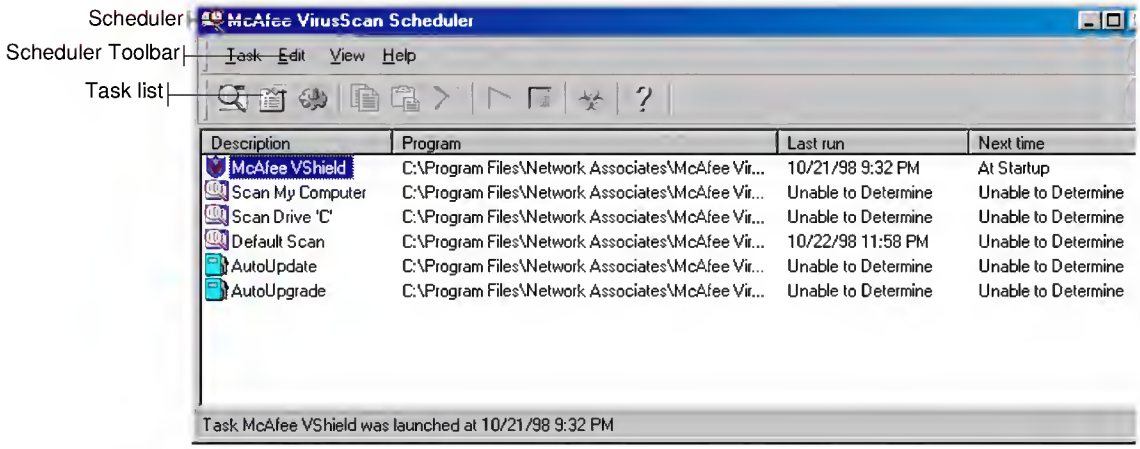

Figure 6-1. VirusScan Scheduler window

The Scheduler window initially shows a list of default tasks that come with the Scheduler, pre-configured and ready to run. A "task" is a set of instructions to run a particular program, in a certain configuration, at a certain time. The Scheduler's task list indicates which program will carry out your task —you'll schedule VShield or SCAN32.EXE for most tasks—displays the time and date when you last ran your task, and shows you when you have it set to run again. Each new task that you create appears at the bottom of the task list.

The toolbar at the top of the Scheduler window gives you quick access to the program's most common commands. To have this toolbar display only its command buttons, click **View**, point to **Toolbar**, then choose **Standard Buttons**. To add text captions to the buttons, click **View**, point to **Toolbar**, then choose **Text Labels**. You can have both options active at the same time—a checkmark beside the menu item indicates which view is active. You'll find most of the same toolbar commands in the menus at the top of the Scheduler window, and in shortcut menus that appear when you click a listed task with your right mouse button.

A status bar at the bottom of the Scheduler window counts the number of listed tasks. When you select a listed task, the status bar tells you when the task last ran. The status bar also shows a brief description of each toolbar button as you pass your mouse cursor over it. Choose **Title Bar** or **Status Bar** from the **View** menu to display or hide each window element.

Using the Scheduler window

From the Scheduler window, you can:

- **Create a new task.** Choose **New Task** from the **Task** menu, or click in the Scheduler toolbar. A Task Properties dialog box will appear. See "Creating new tasks" on page 170 to learn how to specify the actions you want performed.

- **Schedule and enable a task.** Select one of the tasks listed in the Scheduler window, then choose **Properties** from the **Task** menu, or click in the Scheduler toolbar. A Task Properties dialog box will appear. See "Enabling tasks" on page 172 to learn how to specify the options you want for your task and ready it to run.

- **Configure the task program.** Select one of the tasks listed in the Scheduler window, then click in the Scheduler toolbar to display a property page for the VirusScan program component that will run the task. How this property page looks depends on which VirusScan component you run. See "Configuring task options" on page 176 to learn how to choose options for the scan program.

  > **NOTE:** You can configure only those programs that you use to update or upgrade VirusScan or those that perform a scan operation—that is, VShield or VirusScan (SCAN32.EXE). Although you can use VirusScan Scheduler to schedule other programs to run, you cannot use the Scheduler to *configure* other programs.

- **Copy a task.** Select one of the tasks listed in the Scheduler window, then choose **Copy** from the **Edit** menu, or click in the Scheduler toolbar. This copies the task to the Windows clipboard. Next, click inside the Scheduler window, then choose **Paste** from the **Edit** menu, or click in the Scheduler toolbar, to paste a copy of the task to the Scheduler list. Use this feature to copy task settings that you want to use as templates for other, similar tasks.

- **Delete a task.** Select one of the tasks listed in the Scheduler window, then choose **Delete** from the **Task** menu, or click in the Scheduler toolbar.

> **NOTE:** You can delete only tasks that you create—you may not delete any of the tasks from the default set that come with the Scheduler. You can, however, disable any default task that you don't want to run. See "Enabling tasks" on page 172 for details.

- **Start a task.** Select one of the tasks listed in the Scheduler window, then choose **Start** from the **Task** menu, or click in the Scheduler toolbar. The task you selected will start immediately and will run with the options you've chosen. To enable VShield's scanning functions, select McAfee VShield in the task list, then choose **Enable** from the **Task** menu. To start VShield and load it into memory, select the VShield task, then click in the Scheduler toolbar.
- **Stop a task.** Select one of the tasks listed in the Scheduler window, then choose **Stop Now** from the **Task** menu, or click in the Scheduler toolbar. To stop VShield from running, select McAfee VShield in the task list, then click in the Scheduler toolbar. To simply disable VShield, select the VShield task, then choose **Disable** from the **Task** menu. To learn how to stop VShield entirely and remove it from memory, see "Disabling or stopping VShield" on page 132.
- **Connect to the Network Associates Virus Information Library.** Choose **Virus List** from the **View** menu, or click in the Scheduler toolbar. VirusScan will start your preferred browser application and connect to the Network Associates website. See "Viewing File and Virus Information" on page 70 to learn more about what information you'll find in the library.

> **NOTE:** To connect to the Virus Information Library, you must have an Internet connection and web browsing software available on your computer.

- **Open the online help file.** Choose **Help Topics** from the **Help** menu, or click in the Scheduler toolbar to see a list of VirusScan help topics.
- **View an Activity Log.** Select one of the tasks listed in the Scheduler window, then choose **View Activity Log** from the **Task** menu. Not all tasks will have an associated log file, but VirusScan will open the log file for those that do in a Notepad window (see Figure 5-2 on page 142). You can print, edit, copy, or otherwise treat this file as you would any ordinary text file. To learn more about what information each log file records, see Chapter 4, "Using VShield," and Chapter 5, "Using McAfee VirusScan."

- **Start VirusScan Scheduler automatically.** Choose **Load at Startup** from the **View** menu to have the VirusScan Scheduler start whenever you start your computer. The Scheduler has this option enabled by default. Because it must be running in order to execute any tasks you have scheduled, you should choose to have the Scheduler start automatically so that your scheduled tasks will begin at their appointed times.
- **Quit VirusScan Scheduler.** Choose **Exit** from the **Task** menu to quit the Scheduler. If you have any tasks pending, you should minimize the Scheduler rather than quit. To learn how to start the Scheduler again, see "Starting the VirusScan Scheduler" on page 166.

Working with default tasks

As soon as you install VirusScan on your computer and reboot, VShield will immediately begin scanning your system, using a default configuration that provides you with a basic range of protection for your system. The other tasks listed in the Scheduler window also have default configurations set up, but these tasks remain dormant until you activate them. See "Enabling tasks" on page 172 for details.

The default tasks are:

- **VShield.** By default, this task runs automatically as soon as you start your computer. You cannot schedule VShield to run any other time, but you can choose different scan options. See "Setting VShield properties" on page 81 to learn which options you have available.
- **Scan My Computer.** This task scans all fixed disks and all removable media on your system, along with your RAM and hard disk boot sectors. You must activate this task to get it to run. You can run this task in its default configuration or learn how to set your own configuration options for it—see "Configuring VirusScan for scheduled scanning" on page 176.
- **Scan Drive C:.** This task scans your C: drive, your RAM, and the boot sectors of your hard disk by default. You must activate this task to get it to run. You can run this task in its default configuration or learn how to set your own configuration options for it—see "Configuring VirusScan for scheduled scanning" on page 176.
- **Default Scan.** This task serves as a template that you can use to create other tasks. By default, it scans your C: drive, your RAM, and the boot sectors of your disk. You must activate this task to get it to run. You can run this task in its default configuration or learn how to set your own configuration options for it—see "Configuring VirusScan for scheduled scanning" on page 176.

- **AutoUpdate.** This task connects to a server or File Transfer Protocol (FTP) site that you designate to update your VirusScan data (.DAT) files. The task comes configured to connect to a Network Associates server, but you must schedule and activate the task to get it to update your files. You can also configure the task to connect to a central server or FTP site on your network for updated files. See "Configuring AutoUpdate options" on page 196 to learn how to configure this task to suit your needs.
- **AutoUpgrade.** This task connects to a server or FTP site that you designate in order to upgrade your VirusScan program components to their most recent versions. You must configure the task to connect to a particular server or FTP site, then you must schedule and activate the task to get it to upgrade your files. See "Configuring AutoUpgrade options" on page 206 to learn how to configure this task to suit your needs.

Creating new tasks

Although the tasks that come in the default set can provide your system with adequate protection, you will probably want to create and run your own tasks after you have some experience with VirusScan, and have a good idea of what and when you want it to scan.

To create a new task, follow these steps:

1. Choose **New Task** from the **Task** menu in the Scheduler window, or click in the Scheduler toolbar.

   The Task Properties dialog box will appear (Figure 6-2).

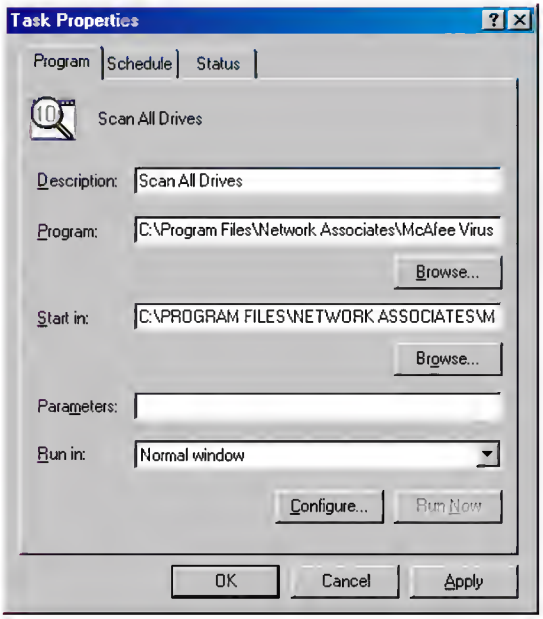

Figure 6-2. Task Properties dialog box - Program page

2. Type a name for the task in the **Description** text box. Be sure that your name describes the task so that you can distinguish it from others in the Scheduler window and so that you can tell at a glance what it does.

3. Type the full path and file name for the program you want to carry out your task in the **Program** text box, or click **Browse** to locate the program on your hard disk.

   By default, the Scheduler chooses VirusScan as the program that will run your task, and locates it in the following path:

   C:\Program Files\Network Associates\McAfee VirusScan\SCAN32.EXE

   You can run any executable program from within the VirusScan Scheduler, but you can configure program options only for VirusScan, VShield, AutoUpdate, and AutoUpgrade. See "Configuring task options" on page 176 for details.

4. To have the program you chose in Step 3 look in a particular folder for its data files, .INI files, or other items that it needs to start, type the path to the correct folder in the **Start In** text box, or click **Browse** to locate it on your hard disk. Ordinarily, a program will look in its own folder for necessary files.

5. Type any parameters you want your program to use when it starts. For most programs, allowable parameters include any options available from the command line, or any files that you want the program to open as it starts.

6. Choose **Normal** from the **Run In** list to have the program appear in its default window when it starts. Choose **Maximized** to expand the window to its largest size. Choose **Minimized** to shrink the window to a taskbar icon.

At this point you have entered enough information to create your task, but you have not yet chosen program options or scheduled it to run. You can

- Click **Apply** to save your changes without closing the Task Properties dialog box, then click the Schedule tab. To learn how to set a task schedule, see "Enabling tasks."
- Click **OK** to save your changes and return to the VirusScan Scheduler window. You will need to set a task schedule later to get it to run. To do so, select the task from the list in the Scheduler window, then click to open the Task Properties dialog box.
- Click **Cancel** to close the dialog box without creating a task.

Enabling tasks

Enabling a task means choosing a schedule for it and activating that schedule so that the task runs when you need it. To run tasks that use VirusScan—not VShield—to scan your system, you'll also need to configure the scan operation to start automatically. See Step 4 on page 183 for more details.

To enable a task, follow these steps:

1. If you do not already have the Task Properties dialog box open, double-click one of the listed tasks in the Scheduler window, or select a task, then click in the Scheduler toolbar.

   The Task Properties dialog box will appear (see Figure 6-2 on page 171). If you chose VShield, AutoUpdate, or AutoUpgrade in the Scheduler task list, the Task Properties dialog box will look a different from that shown in Figure 6-2.

2. Click the Schedule tab to display the correct property page (Figure 6-3).

NOTE: The Task Properties dialog box for VShield will not include a Schedule property page—instead, it will include status pages for each of VShield's scanning modules. The Task Properties dialog boxes for AutoUpdate and AutoUpgrade, meanwhile, will not include status pages.

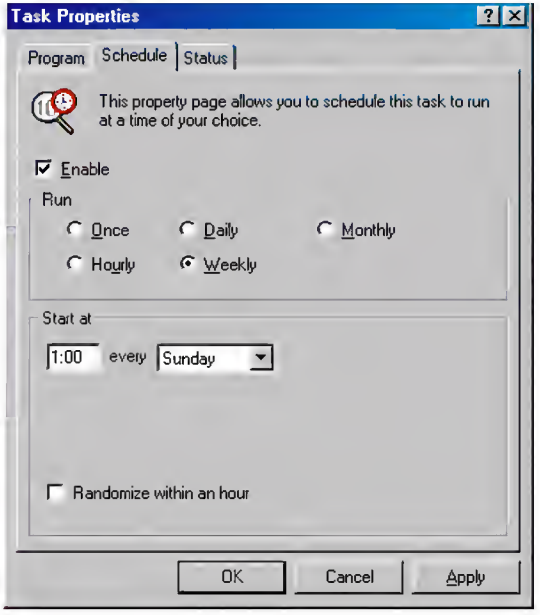

Figure 6-3. Task Properties dialog box - Schedule page

3. Select the **Enable** checkbox. The options in the **Run** and the **Start At** areas become active.

4. Choose how often you want the task to run in the **Run** area. Depending on which interval you select, the **Start At** area gives you a different set of choices for your task schedule. The choices are:

   - **Once.** This runs your task exactly once on the date and at the time you specify. Enter the time in the leftmost text box in the **Start At** area, then select a month from the list to the right. Next, enter the date and the year in the text boxes provided.

   - **Hourly.** This runs your task each hour as long as your computer is on and the Scheduler is running. Specify in the text box provided how many minutes the Scheduler should wait after each hour to run your task.

- **Daily**. This runs your task once at the time you specify on the days you indicate. Enter the time in the text box provided, then select the checkboxes for each day that you want the task to run.
- **Weekly.** This runs your task once each week on the day and at the time you specify. Enter the time in the text box provided, then choose a day from the list to the right.
- **Monthly.** This runs your task once each month on the day and at the time you specify. Enter the time in the leftmost text box, then enter the day of the month on which you want the task to run.

> **NOTE:** Enter all scheduled times, except for the hourly time interval, using a 24-hour clock. If you want the task to run at 9:30 p.m., for example, enter 21:30.

5. Select the **Randomize within an hour** checkbox to have the task start at a random point within 60 minutes of the time you've chosen as its scheduled run time. For example, suppose you've chosen a daily interval and set your task to run at 1:15 a.m. each day. Choosing this option tells the Scheduler to run the task at any random point between 1:15 a.m. and 2:14 a.m.

   With this option activated, you can create and distribute one common VirusScan configuration (.VSC) file across your network, schedule the same set of tasks to run at the same time, yet keep the amount of traffic on your network to a manageable level at any one point. Without this option activated, using the same .VSC file for all computers on your network could cause every computer to activate a scan or update task at the same time, which could drain available network bandwidth.

6. You have now set a schedule for your task and readied it to run at the scheduled time. Click **OK** to close the Task Properties dialog box, or click **Apply** to save your settings without closing the dialog box. Click **Cancel** to close the dialog box without saving your changes.

> **NOTE:** To start your task, your computer must be on and the VirusScan Scheduler must be running. If your computer is off or if the Scheduler is not running at the time your task should start, the task will start at the next scheduled time. You can minimize the Scheduler so that appears only as an icon in the Windows taskbar.
>
> If you plan to have VirusScan run a scan task on an unattended computer, you must also configure the program to start its scan operation automatically. See Step 4 on page 183 for details.

Checking task status

The VirusScan Scheduler window summarizes the time and date when your tasks last ran and when you have scheduled them to start again—look for this information to the right of each listed task. To see the results for each task—how many files it scanned, whether it found any infected files, and what actions it took to respond to the infections—follow these steps to open the Task Properties dialog box to its Status page.

1. If you do not already have the Task Properties dialog box open, double-click one of the listed tasks in the Scheduler window, or select a task, then click in the Scheduler toolbar.
2. The Task Properties dialog box will appear (see Figure 6-2 on page 171). Click the Status tab to display the correct property page (Figure 6-4).

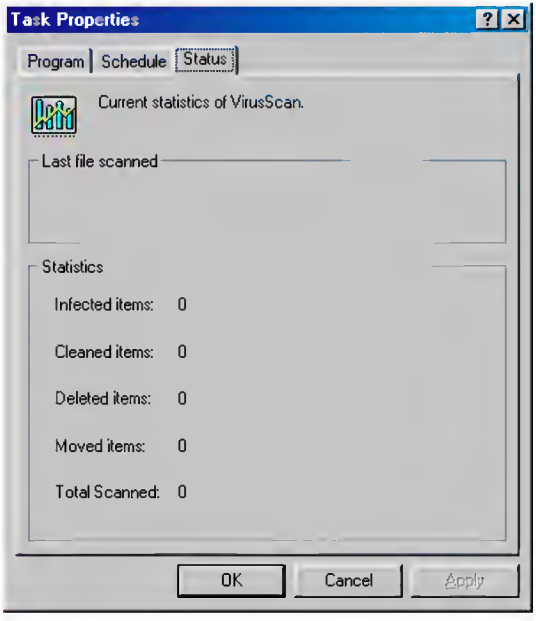

Figure 6-4. Task Properties dialog box - Status page

The status page will list the results of the last scan operation this task conducted, and the name of the last file it scanned. Click **OK** or **Cancel** to close the dialog box.

> **NOTE:** The Task Properties dialog box for the VShield task will include status pages for all of VShield's scanning modules. The Task Properties dialog box for AutoUpdate and AutoUpgrade will not include a status page. To learn more about how to find status information for VShield, see "Tracking VShield status information" on page 136.

Configuring task options

When you first create and schedule a task, the VirusScan Scheduler will run the program that you specify in the Task Properties dialog box with a default set of options. In most cases, the default set will provide your computer with sufficient protection from viruses and other malicious software or will update your data files from the correct server, but you can choose custom options that better reflect your work habits and security needs.

> **NOTE:** You can use the Scheduler to configure VirusScan program components only. To configure any other software that you want to run from within the Scheduler, you must use the tools appropriate for that software to configure it separately. Consult the documentation for your other software for details.
>
> Normally, you'll use VirusScan to perform your scheduled scan tasks. Although you can configure VShield to perform various scan tasks, you cannot specify when it will run—VShield runs when you start your computer and stops running when you shut your computer down. You can disable and re-enable VShield from within the Scheduler, but you cannot create a second VShield task.

Configuring VirusScan for scheduled scanning

To perform a scheduled scan operation, VirusScan needs to know what you want it to scan and what you want it to ignore, what you want it to do if it finds a virus, and how it should let you know when it has. You can also tell VirusScan to keep a record of its actions and prevent others from changing your settings. A series of property pages controls the options for each task—click each tab in the McAfee VirusScan Properties dialog box to set up VirusScan for your task.

To work with the VirusScan property pages, select one of the scan tasks listed in the Scheduler window, then click in the Scheduler toolbar.

NOTE: The task you select must be configured to run VirusScan. You can modify one of the default tasks, or configure a task you created. See "Creating new tasks" on page 170 to learn how to specify the program that will run your scan task.

The McAfee VirusScan Properties dialog box will appear (Figure 6-5).

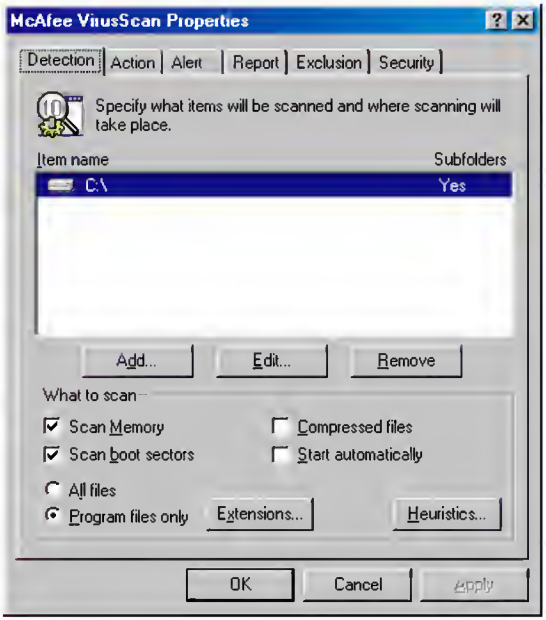

Figure 6-5. VirusScan Properties dialog box - Detection page

Choosing detection options

If you chose to configure a task you just created, VirusScan initially assumes that you want to scan your C: drive and your computer's memory, to look for boot sector viruses, and to restrict the files it scans only to those susceptible to virus infection. If you chose to configure one of the default tasks, your initial options will vary.

To modify the initial task options, follow these steps:

1. Choose which parts of your system or your network that you want VirusScan to examine for viruses. You can

   - **Add scan targets.** Click **Add** to open the Add Scan Item dialog box (Figure 6-6).

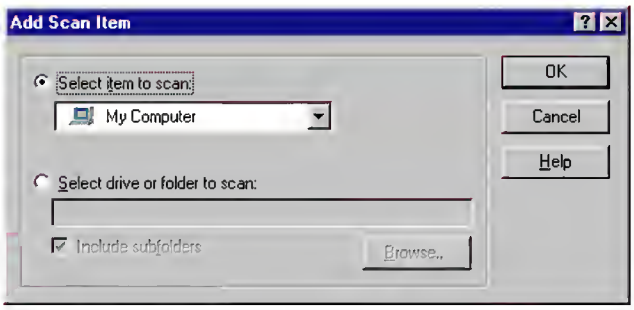

Figure 6-6. The Add Scan Item dialog box

To have VirusScan examine your entire computer or a subset of the drives on your system or your network, click the **Select item to scan** button, then choose the scan target from the list provided. Your choices are:

- **My Computer.** This tells VirusScan to scan all drives physically attached to your computer or logically mapped via Windows Explorer to a drive letter on your computer.
- **All Removable Media.** This tells VirusScan to scan only CD-ROM discs, Syquest and Iomega cartridges, or similar storage devices physically attached to your computer.
- **All Fixed Disks.** This tells VirusScan to scan hard disks physically connected to your computer.
- **All Network Drives.** This tells VirusScan to scan all drives logically mapped via Windows Explorer to a drive letter on your computer.

To have VirusScan examine a particular disk or folder on your system, click the **Select drive or folder to scan** button. Next, in the text box provided, type the drive letter or the path to the folder you want scanned, or click **Browse** to locate the scan target on your computer. Select the **Include subfolders** checkbox to have VirusScan also look for viruses inside any folders within your scan target. Click **OK** to close the dialog box.

- **Change scan targets.** Select one of the listed scan targets, then click **Edit** to open the Edit Item to Scan dialog box (Figure 6-7).

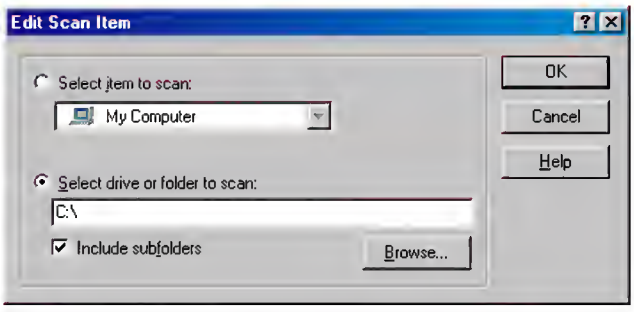

Figure 6-7. The Edit Item to Scan dialog box

The dialog box appears with the existing scan target specified. Choose or enter a new scan target, then click **OK** to close the dialog box.

- **Remove scan targets.** Select one of the listed scan targets, then click **Remove** to delete it.

2. Specify the types of files you want VirusScan to examine. You can

   - **Scan compressed files.** Select the **Compressed files** checkbox to have VirusScan look for viruses in files compressed with these formats: .??_, .CAB, LZEXE, LZH, PKLite, .TD0, and .ZIP. Although it does give you better protection, scanning compressed files can lengthen a scan operation.

   - **Choose file types for scanning.** Viruses ordinarily cannot infect data files or files that contain no executable code. You can, therefore, safely narrow the scope of your scan operations to those files most susceptible to virus infection in order to speed up scan operations. To do so, select the **Program files only** button. To see or designate the file name extensions VirusScan will examine, click **Extensions** to open the Program File Extensions dialog box (Figure 6-8).

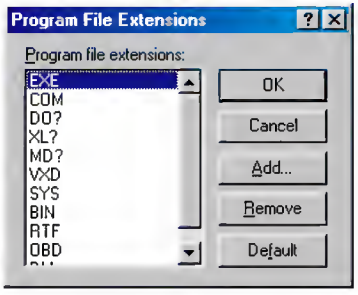

Figure 6-8. The Program File Extensions dialog box

By default, VirusScan looks for viruses in files with the extensions .EXE, .COM, .DO?, .XL?, .RTF, .BIN, .SYS, .MD?, .VXD, .OBD, and .DLL. Files with .DO?, .XL?, .RTF, and .OBD extensions are Microsoft Office files, all of which can harbor macro virus infections. The ? character is a wildcard that enables VirusScan to scan document and template files.

- To add to the list, click **Add**, then type the extensions that you want VirusScan to scan in the dialog box that appears.
- To delete an extension from the list, select it, then click **Remove**.
- Click **Default** to restore the list to its original form.

When you have finished, click **OK** to close the dialog box.

To have VirusScan examine all files on your system, whatever their extensions, select the **All files** button. This will slow your scan operations down considerably, but will ensure that your system is virus free.

- **Turn on heuristic scanning**. Click **Heuristics** to open the Heuristics Scan Settings dialog box (Figure 6-9).

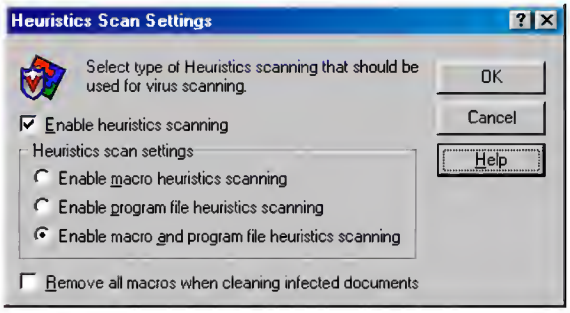
Heuristics Scan Settings
Select type of Heuristics scanning that should be used for virus scanning.
OK
Cancel
Help
Enable heuristics scanning
Heuristics scan settings
Enable macro heuristics scanning
Enable program file heuristics scanning
Enable macro and program file heuristics scanning
Remove all macros when cleaning infected documents

Figure 6-9. Heuristics Scan Settings dialog box

Heuristic scan technology enables VirusScan to recognize new viruses based on their resemblance to similar viruses VirusScan already knows. To do this, the program looks for "virus-like" characteristics in the files you've asked it to scan. The presence of a sufficient number of these characteristics in a file leads VirusScan to identify the file as potentially infected with a new or previously unidentified virus.

Because VirusScan looks simultaneously for file characteristics that rule out the possibility of virus infection, it will rarely give you a false indication of a virus infection. Therefore, unless you know that the file does *not* contain a virus, you should treat "potential" infections with the same caution you would confirmed infections.

To activate heuristic scanning, follow these steps:

a. Select the **Enable heuristics scanning** checkbox. The remaining options in the dialog box activate.

b. Select the types of heuristic scanning you want VirusScan to use. Your choices are:

- **Enable macro heuristics scanning**. Choose this option to have VirusScan identify all Microsoft Word, Microsoft Excel, and other Microsoft Office files that have embedded macros, then compare the macro code to its virus signature database. VirusScan will identify exact matches with the virus name; code signatures that resemble existing viruses cause VirusScan to tell you it has found a potential macro virus.
- **Enable program file heuristics scanning.** Choose this option to have VirusScan locate new viruses in program files by examining their characteristics and comparing them against a list of known virus characteristics. VirusScan will identify files with a sufficient number of these characteristics as potential viruses.
- **Enable macro and program file heuristics scanning.** Choose this option to have VirusScan use both types of heuristic scanning. Network Associates recommends that you use this option for complete anti-virus protection.

c. Determine how you want to treat infected macro files. Select **Remove all macros when cleaning infected documents** to eliminate all infectable code from the document and leave only data. To try to remove only the virus code from the document's macros, leave this checkbox clear.

> **WARNING:** Use this feature with caution: removing all macros from a document can cause it to lose data or to become corrupted and unusable.

d. Click **OK** to save your settings and return to the McAfee VirusScan Properties dialog box.

3. Choose other scanning options. Boot-sector viruses load themselves into your computer's memory and conceal themselves in the boot blocks or master boot record on your hard drive. To detect these viruses, select the **Scan Memory** and **Scan boot sectors** checkboxes.

4. If you have scheduled scan operations that you want to run in your absence, select the **Start automatically** checkbox to tell VirusScan to begin scanning as soon as it launches. If you do not select this checkbox, the Scheduler will start VirusScan, but VirusScan will wait for you to click **Scan Now** to start scanning. Leaving the checkbox clear gives you a chance to cancel the scan operation if it will interfere with your work.

5. Click the Action tab to choose additional VirusScan options. To save your changes without closing the VirusScan Properties dialog box, click **Apply**. To save your changes and return to the Scheduler window, click **OK**. To return to the Scheduler window without saving your changes, click **Cancel**.

> **NOTE:** Clicking **Cancel** will not undo any changes you already saved by clicking **Apply**.

Choosing action options

When VirusScan detects a virus, it can respond either by asking you what it should do with the infected file, or by automatically taking an action that you determine ahead of time. Use the Action property page to specify which response options you want VirusScan to give you when it finds a virus, or which actions you want it to take on its own.

Follow these steps:

1. To start from the Scheduler window, select the task you created in the task list, then click in the Scheduler toolbar.

2. The McAfee VirusScan Properties dialog box appears (see Figure 6-5 on page 178). Click the Action tab to display the correct property page (Figure 6-10).

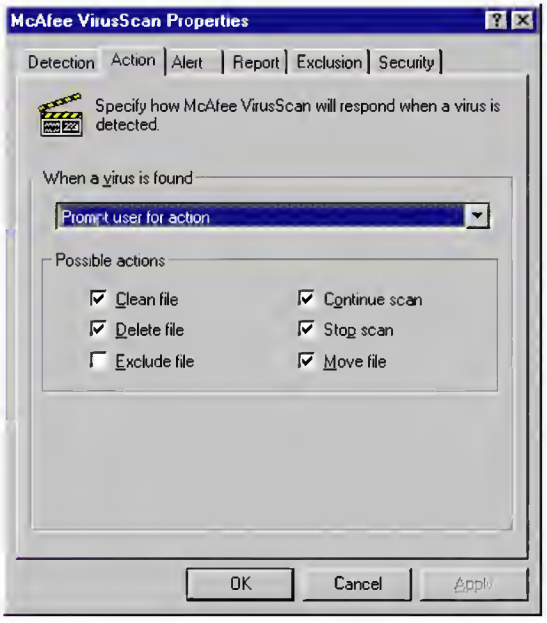

Figure 6-10. VirusScan Properties dialog box - Action page

3. To tell VirusScan what to do when it finds a virus, choose a response from the **When a virus is found** list. The area immediately beneath the list will change to show you additional options for each choice. Your choices are:

   - **Prompt User for Action.** Use this option if you expect to be at your computer when VirusScan examines your disk—the program will display an alert message when it finds a virus and offer you a range of possible responses. Select the response options you want to see in the alert message:

     – **Clean file.** This option tells VirusScan to try to remove the virus code from the infected file.

     – **Delete file.** This option tells VirusScan to delete the infected file immediately.

  - **Exclude file.** This option tells VirusScan to skip the file during later scan operations. This is the only option not selected by default.
  - **Continue scan.** This option tells VirusScan to continue with its scan, but not take any other actions. If you have its reporting options enabled, VirusScan records the incident in its log file.
  - **Stop scan.** This option tells VirusScan to stop the scan operation immediately. To continue, you must restart the operation, either from the Scheduler, or from VirusScan itself.
  - **Move file.** This option tells VirusScan to move the infected file to a quarantine folder.

- **Move infected files automatically**. Use this option to have VirusScan move infected files to a quarantine directory as soon as it finds them. By default, VirusScan moves these files to a folder named INFECTED that it creates at the root level of the drive on which it found the virus. For example, if VirusScan found an infected file in T:\MY DOCUMENTS and you specified INFECTED as the quarantine directory, VirusScan would copy the file to T:\INFECTED.

  You can enter a different name in the text box provided, or click **Browse** to locate a suitable folder on your hard disk.

- **Clean infected files automatically.** Use this option to tell VirusScan to remove the virus code from the infected file as soon as it finds it. If VirusScan cannot remove the virus, it will notify you in its message area and, if you have its reporting features enabled, will note the incident in its log file. See "Choosing report options" on page 188 for details.

- **Delete infected files automatically.** Use this option to have VirusScan delete every infected file it finds immediately. Be sure to enable its reporting feature so that you have a record of which files VirusScan deleted. You will need to restore deleted files from backup copies.

- **Continue scanning.** Use this option only if you plan to leave your computer unattended while VirusScan checks for viruses. If you also activate the VirusScan reporting feature (see "Choosing report options" on page 188 for details), the program will record the names of any viruses it finds and the names of infected files so that you can delete them at your next opportunity.

4. Click the Alert tab to choose additional VirusScan options. To save your changes without closing the VirusScan Properties dialog box, click **Apply**. To save your changes and return to the Scheduler window, click **OK**. To return to the Scheduler window without saving your changes, click **Cancel**.

> **NOTE:** Clicking **Cancel** will not undo any changes you already saved by clicking **Apply**.

Choosing alert options

Once you configure VirusScan with the response options you want, you can let it look for and remove viruses from your system automatically, as it finds them, with almost no further intervention. If, however, you want VirusScan to inform you immediately when it finds a virus so that you can take appropriate action, you can configure it to send an alert message to you in a variety of ways. Use the Alert property page to choose which alerting methods you want to use.

Follow these steps:

1. To start from the Scheduler window, select the task you created in the task list, then click in the Scheduler toolbar.
2. The McAfee VirusScan Properties dialog box appears (see Figure 6-5 on page 178). Click the Alert tab to display the correct property page (Figure 6-11).

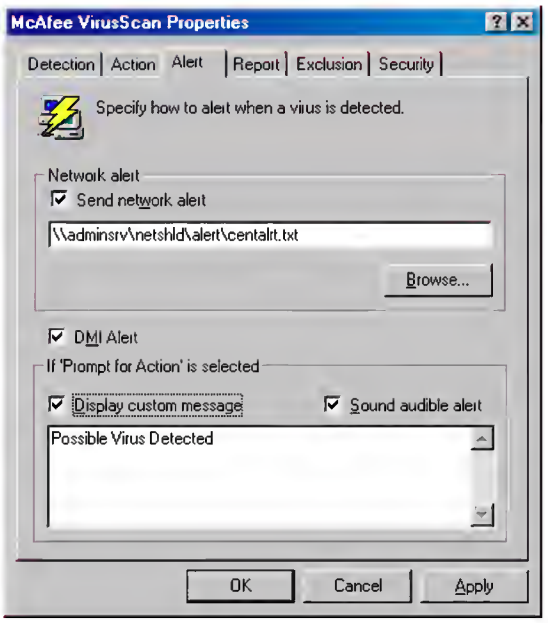

Figure 6-11. VirusScan Properties dialog box - Alert page

3. To tell VirusScan to send an alert message to a server running NetShield, a Network Associates server-based anti-virus solution, select the **Send network alert** checkbox, then enter the path to the NetShield alert folder on your network, or click **Browse** to locate the correct folder.

   NOTE: The folder you choose must contain CENTALRT.TXT, the NetShield Centralized Alerting file. NetShield collects alert messages from VirusScan and other Network Associates software, then passes them to network administrators for action. To learn more about Centralized Alerting, see the NetShield *User's Guide*.

4. To have VirusScan send virus alert messages via the DMI Component Interface to desktop and network management applications running on your network, select the **DMI Alert** checkbox.

   NOTE: The Desktop Management Interface is a standard for communicating management requests and alert information between hardware and software components stored on or connected to desktop computers, and the applications used for managing them. To learn more about using this alert method, see your network administrator.

5. If you chose **Prompt user for action** as your response in the Action page (see "Choosing action options" on page 183 for details), you can also tell VirusScan to beep and display a custom message when it finds a virus. To do so, select the **Display custom message** checkbox, then enter the message you want to see in the text box provided—you can enter a message of up to 225 characters in length. Next, select the **Sound audible alert** checkbox.

6. Click the Report tab to choose additional VirusScan options. To save your changes without closing the VirusScan Properties dialog box, click **Apply**. To save your changes and return to the Scheduler window, click **OK**. To return to the Scheduler window without saving your changes, click **Cancel**.

> **NOTE:** Clicking **Cancel** will not undo any changes you already saved by clicking **Apply**.

Choosing report options

VirusScan lists its current settings and summarizes all of the actions it takes during its scanning operations in a log file called VSCLOG.TXT. You can have VirusScan write its log to this file, or you can use any text editor to create a text file for VirusScan to use. You can then open and print the log file for later review from within VirusScan or from a text editor.

The VSCLOG.TXT file can serve as an important management tool for you to track virus activity on your system and to note which settings you used to detect and respond to the infections VirusScan found. You can also use the incident reports recorded in the file to determine which files you need to replace from backup copies, examine in quarantine, or delete from your computer. Use the Reports property page to determine which information VirusScan will include in its log file.

To set VirusScan to record its actions in a log file, follow these steps:

1. To start from the Scheduler window, select the task you created in the task list, then click in the Scheduler toolbar.

2. The McAfee VirusScan Properties dialog box appears (see Figure 6-5 on page 178). Click the Report tab to display the correct property page (Figure 6-12).

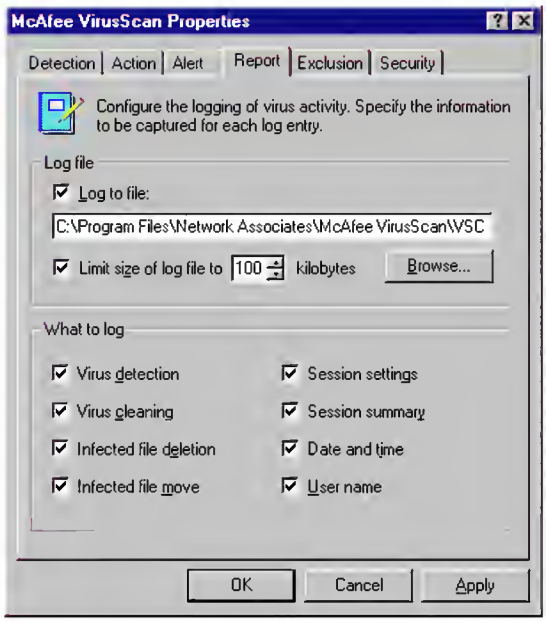

Figure 6-12. VirusScan Properties - Reports page

3. Select the **Log to file** checkbox.

   By default, VirusScan writes log information to the file VSCLOG.TXT in the VirusScan program directory. You can enter a different name in the text box provided, or click **Browse** to locate a suitable file elsewhere on your hard disk or on your network.

4. To minimize the log file size, select the **Limit size of log file to** checkbox, then enter a value for the file size, in kilobytes, in the text box provided.

   Enter a value between 10KB and 999KB. By default, VirusScan limits the file size to 100KB. If the data in the log exceeds the file size you set, VirusScan erases the existing log and begins again from the point at which it left off.

5. Select the checkboxes that correspond to the information you want VirusScan to record in its log file. You can choose to record any of this information:

   - **Virus detection.** Select this checkbox to have VirusScan note the number of infected files it found during this scanning session.
   - **Virus cleaning.** Select this checkbox to have VirusScan note the number of infected files from which it removed the infecting virus.
   - **Infected file deletion.** Select this checkbox to have VirusScan note the number of infected files it deleted from your system.
   - **Infected file move.** Select this checkbox to have VirusScan note the number of infected files it moved to your quarantine directory.
   - **Session settings.** Select this checkbox to have VirusScan list the options you choose in the McAfee VirusScan Properties dialog box for each scanning session.
   - **Session summary.** Select this checkbox to have VirusScan summarize its actions during each scanning session. Summary information includes the number of files scanned, the number and type of viruses detected, the number of files moved or deleted, and other information.
   - **Date and time.** Select this checkbox to have VirusScan append the date and time to each log entry it records.
   - **User name.** Select this checkbox to have VirusScan append the name of the user logged in to your computer at the time it records each log entry.

   To see the contents of the log file from VirusScan Scheduler, select the task you created in the task list, then choose **View Activity Log** from the **Task** menu. You can also start VirusScan and choose **View Activity Log** from the **File** menu. For more information, see "Using VirusScan menus" on page 141.

6. Click the Exclusion tab to choose additional VirusScan options. To save your changes without closing the VirusScan Properties dialog box, click **Apply**. To save your changes and return to the Scheduler window, click **OK**. To return to the Scheduler window without saving your changes, click **Cancel**.

   ☐ **NOTE:** Clicking **Cancel** will not undo any changes you already saved by clicking **Apply**.

Choosing exclusion options

Many of the files stored on your computer are not vulnerable to virus infection. Scan operations that examine these files can take a long time and produce few results. You can speed up scan operations by telling VirusScan to look only at susceptible file types (see "Choosing detection options" on page 178 for details), or you can tell VirusScan to ignore entire files or folders that you know cannot become infected.

Once you scan your system thoroughly, you can exclude the files and folders that do not change or that are not normally vulnerable to virus infection. You can also rely on VShield to provide you with protection in between scheduled scan operations. Regular scan operations that examine all areas of your computer, however, provide you with the best virus defense.

To exclude files or folders from scan operations, follow these steps:

1. To start from the Scheduler window, select the task you created in the task list, then click in the Scheduler toolbar.
2. The McAfee VirusScan Properties dialog box appears (see Figure 6-5 on page 178). Click the Exclusion tab to display the correct property page. (Figure 6-13).

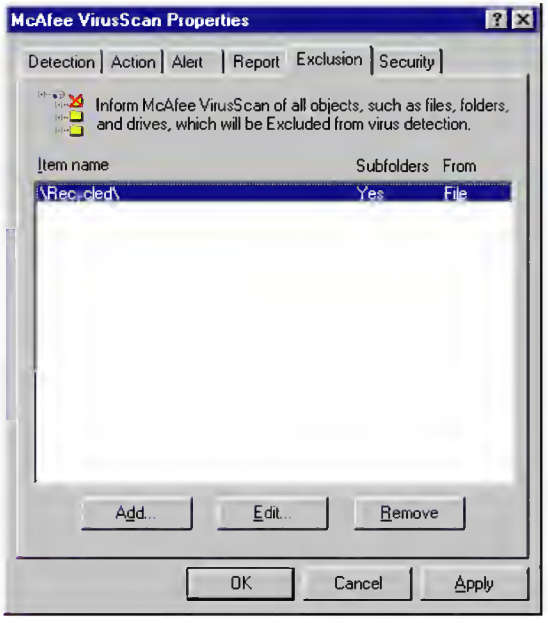

Figure 6-13. VirusScan Properties dialog box - Exclusion page

The Exclusion page will initially list only your Recycle Bin. VirusScan excludes the Recycle Bin from scan operations because Windows will not run files stored there.

3. Specify the items you want to exclude. You can

   - **Add files, folders or volumes to the exclusion list.** Click **Add** to open the Add Exclude Item dialog box (Figure 6-14).

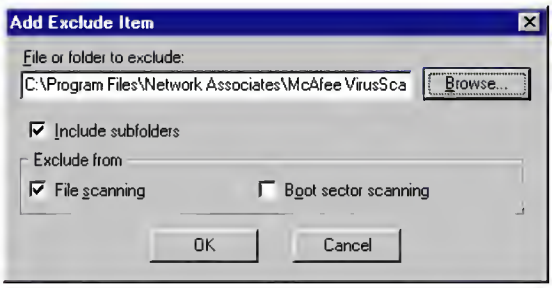

Figure 6-14. Add Exclude Item dialog box

   a. Type the volume, the path to the file, or the path to the folder that you want to exclude from scanning, or click **Browse** to locate a file or folder on your computer.

      NOTE: If you have chosen to move infected files to a quarantine folder automatically, the program excludes that folder from scan operations.

   b. Select the **Include Subfolders** checkbox to exclude all subfolders within the folder you just specified.

   c. Select the **File scanning** checkbox to tell VirusScan not to look for file-infector viruses in the files or folders you exclude.

   d. Select the **Boot sector scanning** checkbox to tell VirusScan not to look for boot-sector viruses in the files or folders you exclude. Use this option to exclude system files, such as COMMAND.COM, from scan operations.

      WARNING: Network Associates recommends that you do *not* exclude your system files from virus scanning.

   e. Click **OK** to save your changes and close the dialog box.

   f. Repeat steps a. through d. until you have listed all of the files and folders that you do not want scanned.

- **Change the exclusion list.** To change the settings for an exclusion item, select it in the Exclusions list, then click **Edit** to open the Edit Exclude Item dialog box. Make the changes you need, then click **OK** to close the dialog box.
- **Remove an item from the list.** To delete an exclusion item, select it in the list, then click **Remove**. VirusScan will then scan this file or folder during its next scanning operation.

4. Click the Security tab to choose additional VirusScan options. To save your changes without closing the VirusScan Properties dialog box, click **Apply**. To save your changes and return to the Scheduler window, click **OK**. To return to the Scheduler window without saving your changes, click **Cancel**.

> **NOTE:** Clicking **Cancel** will not undo any changes you already saved by clicking **Apply**.

Choosing security options

VirusScan lets you set a password to protect the settings you choose in each property page from unauthorized changes. This feature is particularly useful for system administrators who need to keep users from tampering with their security measures by changing VirusScan settings. Use the Security property page to lock your settings.

Follow these steps:

1. To start from the Scheduler window, select the task you created in the task list, then click in the Scheduler toolbar.
2. The McAfee VirusScan Properties dialog box appears (see Figure 6-5 on page 178). Click the Security tab to display the correct property page. (Figure 6-15).

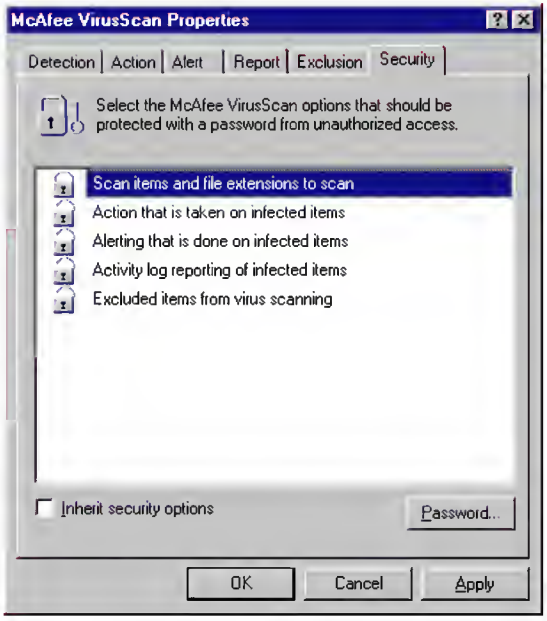

Figure 6-15. VirusScan Properties dialog box - Security page

3. Select the settings you want to protect in the list shown.

   You may protect any or all VirusScan property pages. Protected property pages display a locked padlock icon in the security list shown in Figure 6-15. To remove protection from a property page, click the locked padlock icon to unlock it.

4. Click **Password** to open the Specify Password dialog box (Figure 6-16).

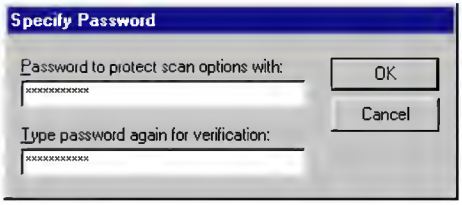

Figure 6-16. Specify Password dialog box

   a. Enter a password in the first text box shown, then enter the same password again in the text box below to confirm your choice.

   b. Click **OK** to close the Specify Password dialog box.

5. If you want to create other scan tasks by copying this task (see page 167 for details), you can ensure that your security settings will appear by default in the copied task by selecting the **Inherit security options** checkbox. If you configure the Default Scan task with this option, all new tasks you create by choosing **New Task** from the **Scan** menu or by clicking will have the security settings you choose for the Default Scan task.

6. Click a different tab to change any of your VirusScan settings. To save your changes without closing the VirusScan Properties dialog box, click **Apply**. To save your changes and return to the Scheduler window, click **OK**. To return to the Scheduler window without saving your changes, click **Cancel**.

> **NOTE:** Clicking **Cancel** will not undo any changes you already saved by clicking **Apply**.

Configuring AutoUpdate options

To function at peak efficiency, VirusScan needs regular infusions of new virus definition files, updates to its database of harmful objects and Internet sites, and other technical enhancements. Without updated files, VirusScan might not recognize new forms of malicious software or detect new virus strains when it encounters them.

Network Associates, through its McAfee Labs division, updates these critical files regularly and frequently, and makes the revised files available on its FTP (File Transfer Protocol) servers as data file (.DAT) packages. A .DAT package consists of an archived .ZIP file named DAT-XXXX.ZIP. The XXXX in the file name is a series number that changes with each .DAT file release.

NOTE: "Updating" VirusScan means downloading and installing new .DAT file versions; "upgrading" VirusScan means downloading and installing product version revisions, executables and, in some cases, .DAT files. Network Associates offers free .DAT file updates for the life of your product. This does not, however, guarantee that .DAT files will be compatible with previous product versions.

Your right to download free VirusScan upgrades depends on the terms of your license or on the terms of the sales contract you agreed to at the time of your purchase. If you have questions about these terms, consult the LICENSE.TXT or README.1ST documents included with your VirusScan copy , or consult your sales representative. Network Associates makes upgrade files available for you to download freely from its FTP sites and other services for as long as your license permits. VirusScan Scheduler uses a different task, AutoUpgrade, to control when and how often you download new VirusScan files. See "Configuring AutoUpgrade options" on page 206 to learn how to configure this task.

By default, the AutoUpdate task included with VirusScan Scheduler comes configured to download the most recent .DAT file updates directly from the Network Associates FTP site. This configuration can make administration simple and straightforward for small networks or individual VirusScan installations. If you have a large network, however, retaining this configuration can severely tax your external bandwidth if, as will happen if you leave the default configuration enabled, each network node tries to update its .DAT files at once.

Instead, Network Associates recommends using AutoUpdate in conjunction with its companion service, Enterprise SecureCast, in an efficient "push-pull" arrangement. Once you install its client software on an administrative server, SecureCast can send, or "push," updated files to you automatically, as soon as McAfee Labs makes them available. See "Setting up Enterprise SecureCast" on page 251 for more details.

If you then make these updated files available on one or more central servers on your network and configure your remaining network nodes to "pull" the updated files from those servers, you can

- Schedule network-wide .DAT file roll-outs for convenient times and with minimal intervention from either administrators or network users. With VirusScan Scheduler's Task Properties dialog box, you can determine when each network node will poll the server for updated files.

  You might, for example, specify one convenient update time when you first deploy VirusScan, but set AutoUpdate to trigger at a random interval within 60 minutes of that time, or set a schedule that phases in or rotates .DAT file updates among different parts of the network. To learn how to schedule AutoUpdate or other tasks, see "Enabling tasks" on page 172.

- Split roll-out administration duties among different servers or domain controllers, among different regions of wide-area networks, or across other network divisions. Keeping update traffic primarily internal can also reduce the potential for network security breaches.

- Reduce the likelihood that you will need to wait to download new .DAT files. Traffic on Network Associates servers increases dramatically on regular .DAT file publishing dates. Avoiding the competition for network bandwidth enables you to deploy your update with minimal interruptions.

Other advanced AutoUpdate options allow you to back up existing .DAT files, install the .DAT file update, reboot the updated computer, if necessary, or run particular programs after successful updates. A set of AutoUpdate property pages controls the options for this task—click each tab in the Automatic Update Properties dialog box to configure them.

To configure AutoUpdate, follow these steps:

1. Select the AutoUpdate task shown in the Scheduler window, then click in the Scheduler toolbar.

   NOTE: AutoUpdate runs according to the schedule you set for it in its Task Properties dialog box. To open the Task Properties dialog box instead, select the AutoUpdate task, then click in the Scheduler toolbar. To learn more about setting a task schedule, see "Enabling tasks" on page 172.

   The Automatic Update dialog box will appear (see Figure 6-17 on page 198).

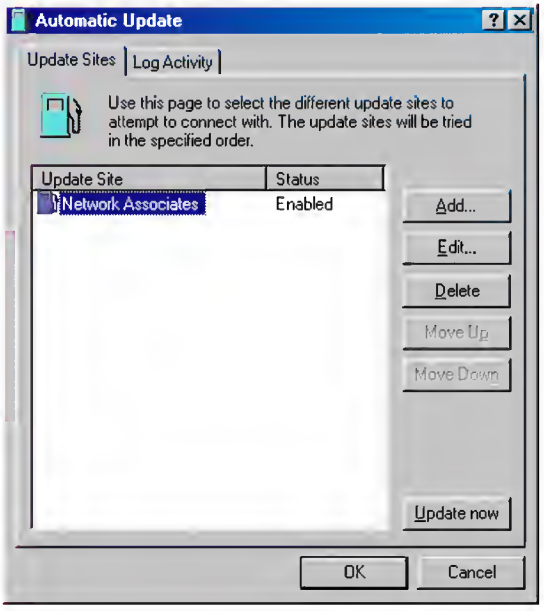

Figure 6-17. Automatic Update dialog box - Update Sites page

Here, AutoUpdate lists the sites from which it will download new .DAT files. Initially, AutoUpdate comes configured to connect only to the Network Associates FTP site. You can add as many different sites as you need, and alter the order in which AutoUpdate tries to connect to them, from this dialog box. Your options are:

- **Add a new site.** Click **Add** to open the Automatic Update Properties dialog box (Figure 6-18). To learn how to specify options for your new site, see "Configuring update options" on page 201.

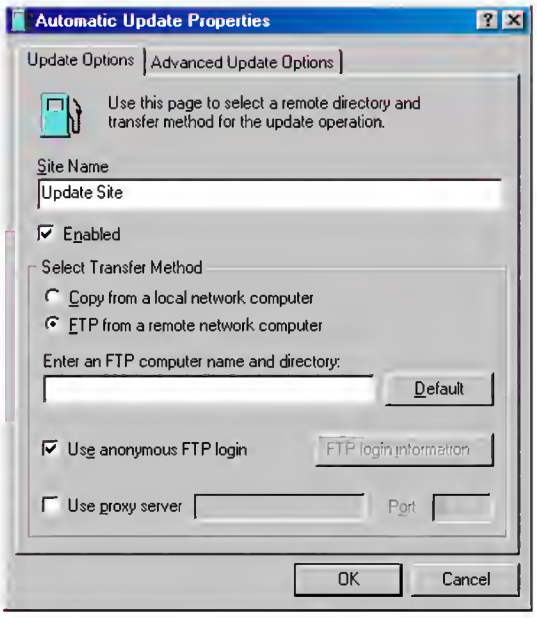

Figure 6-18. Automatic Update Properties dialog box - Update Options page

- **Change the options for an existing site.** Select one of the sites shown in the list, then click **Edit** to open the Automatic Update Properties dialog box (see Figure 6-18 on page 199). Make the changes you want to make, then click **OK** to close the dialog box. To see descriptions and instructions for configuring the available options, see "Configuring update options" on page 201.
- **Remove an existing site.** Select one of the sites shown in the list, then click **Delete** to remove it.
- **Change the search order for existing sites.** To change the order in which AutoUpdate connects to the sites listed in the dialog box, select the site whose priority you want to change, then click **Move Up** to give the site a higher priority, or **Move Down** to give it a lower priority.
- **Update your .DAT files immediately.** Click **Update Now** to have AutoUpdate connect immediately to the first site listed and check for new .DAT files. To use this function, you must have configured enough of the necessary options for AutoUpdate to locate the listed site and, if necessary, log on to it. See "Configuring update options" on page 201 to learn how to specify the options you need.

If AutoUpdate cannot connect to the listed site after three attempts, or if it does not find new .DAT files, it will connect to each of the other sites listed until it finds the most current .DAT files available. If you have the **Force Update** option selected, AutoUpdate will download any .DAT files it finds on the first site to which it can connect successfully. See "Configuring advanced update options" on page 203 for more details.

2. Click the Log Activity tab to display the next property page (Figure 6-19).

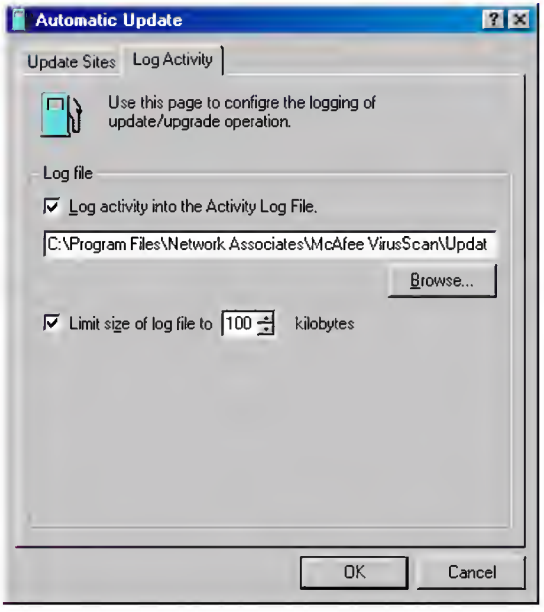

Figure 6-19. Automatic Update dialog box - Log Activity page

3. Select the **Log activity into the Activity Log File** checkbox.

   By default, AutoUpdate records what happens during update attempts and saves the record in the file UPDATE UPGRADE ACTIVITY LOG.TXT in the VirusScan program directory. You can enter a different name and path in the text box provided, or click **Browse** to locate a suitable file elsewhere on your hard disk or on your network.

4. To minimize the log file size, select the **Limit size of log file to** checkbox, then enter a value for the file size, in kilobytes, in the text box provided.

Enter a value between 10KB and 999KB. By default, AutoUpdate limits the file size to 100KB. If the data in the log exceeds the file size you set, AutoUpdate erases the existing log and begins again from the point at which it left off. To see the contents of the log file from VirusScan Scheduler, select the AutoUpdate task in the task list, then choose **View Activity Log** from the **Task** menu.

5. Click **OK** to save your changes and close the Automatic Update dialog box. Click **Cancel** to close the dialog box without saving your changes. AutoUpdate saves all of the changes you make in the Automatic Update dialog box to UPDATE.INI, a file stored in the VirusScan program directory. To replicate these same settings across your network, copy UPDATE.INI to the VirusScan program directory on each network node.

Configuring update options

To create a new update site or change the settings for an existing site, click **Add** in the Automatic Update dialog box (see Figure 6-17 on page 198), or select a listed site, then click **Edit**. Either action will open the Automatic Update Properties dialog box (Figure 6-20).

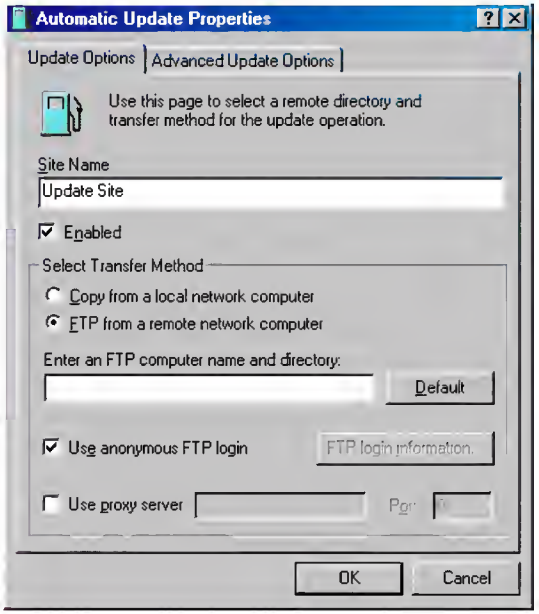

Figure 6-20. Automatic Update Properties dialog box - Update Options page

Next, follow these steps:

1. Type a name for the site in the text box provided. Choose a descriptive name that you will recognize in the site list.
2. Click **Enabled** to tell AutoUpdate to connect to this site at the time you have scheduled. Clearing the checkbox preserves the options you have configured, but tells AutoUpdate not to check the site.

   AutoUpdate will make a maximum of three connection attempts for the site during each scheduled update operation. When it does connect and download the new .DAT file package, AutoUpdate also extracts the files and installs them into the VirusScan program directory.
3. Choose the method you want to use to connect to the target server. Your choices are:

   - **Copy from a local network computer**. Select this option to simply transfer the update files from a computer somewhere on your network via whichever common network protocol you have active. The settings for this protocol will govern how AutoUpdate attempts the connection and the length of the timeout period that must pass before AutoUpdate stops the connection attempt.

     Enter the computer name in Universal Naming Convention (UNC) notation in the text box provided, or click **Browse** to locate the computer on your network. The remaining options in the dialog box become unavailable.

   - **FTP from a remote network computer**. Select this option to transfer the update files via File Transfer Protocol (FTP). To use this option, the target server must have an FTP service enabled.

     AutoUpdate uses its own FTP implementation to connect to the server, but the timeout period for the connection attempt will depend on your existing network protocol settings.

     Next, enter the domain name for the target server, together with any other necessary directory information, in the text box provided. Clicking **Default** enters the Network Associates FTP server.

     If the target server accepts anonymous FTP logins, select the **Use anonymous FTP login** checkbox. If you use a specific FTP account that requires a user name and password, clear the checkbox, then click **FTP login information** instead. This button opens a dialog box where you can enter the correct user name and password. Enter the password again to confirm it, then click **OK** to close the dialog box.

4. If you route FTP requests from your network through a proxy server, select the **Use proxy server** checkbox, then enter the name of your proxy server in the text box provided. You can enter the name in UNC notation or as a domain name, whichever is appropriate for your environment. Next, in the remaining text box, enter the logical port for the proxy server that AutoUpdate should address with its FTP request.

5. To choose additional options, click the Advanced Update tab. To save your changes and return to the Automatic Update dialog box, click **OK**. AutoUpdate saves all of the changes you make in the Automatic Update dialog box to UPDATE.INI, a file stored in the VirusScan program directory. To close the dialog box without saving your changes, click **Cancel**.

Configuring advanced update options

To complete your AutoUpdate task, you need to enter only a target server, a connection method, and any necessary login information. Then, once you enable the task and set a schedule for it, AutoUpdate will download the correct files from the target server for you, extract them from their .ZIP archives, and install them into the VirusScan program directory.

To have AutoUpdate do additional pre- or post-processing on the files, or to have it take other actions, click the Advanced Update Options tab to display the correct property page (Figure 6-21).

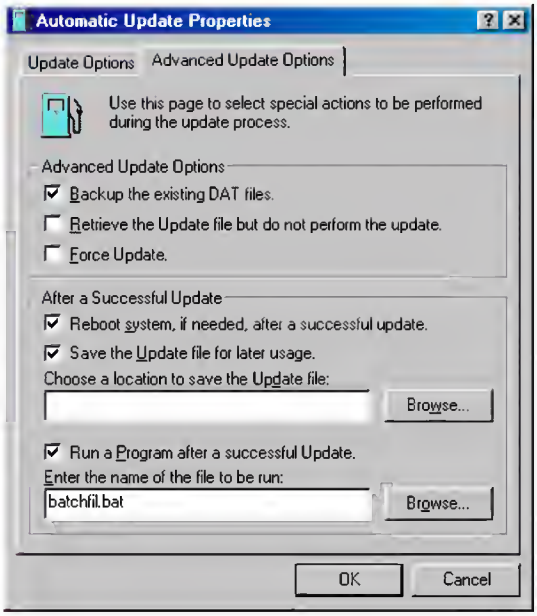
Automatic Update Properties
Update Options
Advanced Update Options
Use this page to select special actions to be performed during the update process.
Advanced Update Options
Backup the existing DAT files.
Retrieve the Update file but do not perform the update.
Force Update.
After a Successful Update
Reboot system, if needed, after a successful update.
Save the Update file for later usage.
Choose a location to save the Update file:
Browse...
Run a Program after a successful Update.
Enter the name of the file to be run:
batchfil.bat
Browse...
OK
Cancel

Figure 6-21. Automatic Update Properties dialog box - Advanced Update Options page

Next, follow these steps:

1. Tell AutoUpdate what you want it to do before or as it performs an update. Your options are:

   - **Backup the existing .DAT files.** Select this checkbox to have AutoUpdate rename existing VirusScan .DAT files before it installs new files. To rename each file, AutoUpdate appends the extension .SAV to the existing file name and extension. CLEAN.DAT, for example, will become CLEAN.DAT.SAV.

   - **Retrieve the Update file but do not perform the update**. Select this checkbox to have AutoUpdate download the .ZIP archive that contains the new .DAT files and simply save it in a location you specify instead of extracting it and installing it.

     Selecting this checkbox also selects the **Save the Update file for later usage** checkbox in the **After a Successful Update** area. To tell AutoUpdate where to save the .DAT file package, enter a path and folder name in the text box below this checkbox, or click **Browse** to locate a suitable folder.

     You might want to use this option if you download new .DAT files to a central server on your network and want individual client computers to download, extract and install the new files locally.

   - **Force Update.** Select this checkbox to tell AutoUpdate to download and install whichever .DAT file package it finds on the target server, whether that package is more recent than your existing .DAT files or not. You might use this option to "refresh" .DAT files stored in your VirusScan program directory periodically, in case your existing files have become corrupted. This option will also circumvent any error messages that VirusScan might return if it doesn't find new files on the target server at the time you have your update task scheduled.

     WARNING: Network Associates recommends that you use this option with extreme caution. If your AutoUpdate task is configured to connect to a server that stores older .DAT file versions, you can reduce VirusScan's effectiveness and expose your computer or network to infection from newly emerging viruses and other malicious software. Upgrades to VirusScan program components can also cause incompatibilities with older .DAT file versions. These incompatibilities can, in turn, cause VirusScan to behave unpredictably.

2. Tell AutoUpdate what you want it to do after it successfully downloads, extracts, and installs new .DAT files. Your options are:

   - **Reboot system, if needed, after a successful update**. Select this checkbox to have AutoUpdate restart your system after it installs new .DAT files.

     Although VirusScan and VShield need you to restart your system in order load new .DAT files, you might want to do so only during idle hours so as not to interfere with productive work. If you plan to run a program after updating your .DAT files, you should leave this checkbox clear.

     NOTE: This option functions only for scheduled update operations. If you click **Update Now** in the Automatic Update dialog box, AutoUpdate will ask you if you want to restart your computer as soon as it finishes installing new .DAT files , whether you selected this option or not.

   - **Save the Update file for later usage.** Select this checkbox to have AutoUpdate save an unextracted copy of the .DAT file package in a location you specify. AutoUpdate then extracts the .DAT files from the update package and continues with the installation. By contrast, the **Retrieve the Update file but do not perform the update** option saves the unextracted file, but does not install the new .DAT files.

     To tell AutoUpdate where to save the .DAT file package, enter a path and folder name in the text box below this checkbox, or click **Browse** to locate a suitable folder.

   - **Run a Program after a successful Update.** Select this checkbox to tell AutoUpdate to start another program after it finishes installing new .DAT files. You might want to use this option, for example, to start an e-mail client program or a network message utility that notifies a system administrator that the update operation completed successfully.

     Next, enter the path and file name for the program you want to run, or click **Browse** to locate the program on your hard disk.

3. To save your changes and return to the Automatic Update dialog box, click **OK**. AutoUpdate saves all of the changes you make in the Automatic Update dialog box to UPDATE.INI, a file stored in the VirusScan program directory. To close the dialog box without saving your changes, click **Cancel**.

Configuring AutoUpgrade options

Network Associates revises VirusScan frequently to add new detection and repair capabilities, new features for manageability and flexibility, and other enhancements that make it a better anti-virus security tool. VirusScan's AutoUpgrade utility is designed specifically to look for and download these new versions as they become available.

NOTE: "Updating" VirusScan means downloading and installing new .DAT file versions; "upgrading" VirusScan means downloading and installing product version revisions, executables and, in some cases, .DAT files. Network Associates offers free .DAT file updates for the life of your product. This does not, however, guarantee that .DAT files will be compatible with previous product versions.

Your right to download free VirusScan upgrades depends on the terms of your license or on the terms of the sales contract you agreed to at the time of your purchase. If you have questions about these terms, consult the LICENSE.TXT or README.1ST documents included with your VirusScan copy , or consult your sales representative. Network Associates makes upgrade files available for you to download freely from its FTP sites and other services for as long as your license permits. VirusScan Scheduler uses a different task, AutoUpgrade, to control when and how often you download new VirusScan files. See "Configuring AutoUpgrade options" on page 206 to learn how to configure this task.

By default, the AutoUpgrade task included with VirusScan Scheduler does not come configured with the site information necessary to download new VirusScan versions. Registered VirusScan users can obtain this information from their sales representatives or from other Network Associates sources.

Network Associates recommends using AutoUpgrade in conjunction with its companion service, Enterprise SecureCast, in an efficient "push-pull" arrangement. Once you install its client software on an administrative server, SecureCast can send, or "push," updated VirusScan files to you automatically, as soon as Network Associates makes them available. See "Setting up Enterprise SecureCast" on page 251 for more details.

If you then make these updated files available on one or more central servers on your network and configure your remaining network nodes to "pull" the updated files from those servers, you can

- Schedule network-wide roll-outs of new VirusScan versions for convenient times and with minimal intervention from either administrators or network users. With VirusScan Scheduler's Task Properties dialog box, you can determine when each network node will poll the server for updated files.

You might, for example, specify one convenient time to run AutoUpgrade when you first deploy VirusScan, but set it to trigger at a random interval within 60 minutes of that time, or set a schedule that phases in or rotates upgrade roll-outs among different parts of the network. To learn how to schedule AutoUpgrade or other tasks, see "Enabling tasks" on page 172.

- Split roll-out administration duties among different servers or domain controllers, among different regions of wide-area networks, or across other network divisions. Keeping update traffic primarily internal can also reduce the potential for network security breaches.
- Reduce the likelihood that you will need to wait to download new VirusScan versions. Traffic on Network Associates servers increases dramatically when new VirusScan versions are released. Avoiding the competition for network bandwidth enables you to deploy new versions with minimal interruptions.

> **IMPORTANT:** If you store new VirusScan upgrade files on a server that uses case-sensitive file names, you must rename the file PKGDESC.INI, which comes with VirusScan upgrades, so that it uses only lower-case letters. Otherwise, AutoUpgrade will not find the file on the server and therefore will not install the new VirusScan version on client computers.

Other advanced AutoUpgrade options allow you to reboot your system or save the upgrade package for later use. A set of AutoUpgrade property pages controls the options for this task—click each tab in the Automatic Upgrade Properties dialog box to configure them.

To configure AutoUpgrade, follow these steps:

1. Select the AutoUpgrade task shown in the Scheduler window, then click in the Scheduler toolbar.

   > **NOTE:** AutoUpgrade runs according to the schedule you set for it in its Task Properties dialog box. To open the Task Properties dialog box instead, select the AutoUpgrade task, then click in the Scheduler toolbar. To learn more about setting a task schedule, see "Enabling tasks" on page 172.

   The Automatic Upgrade dialog box will appear (see Figure 6-22 on page 208).

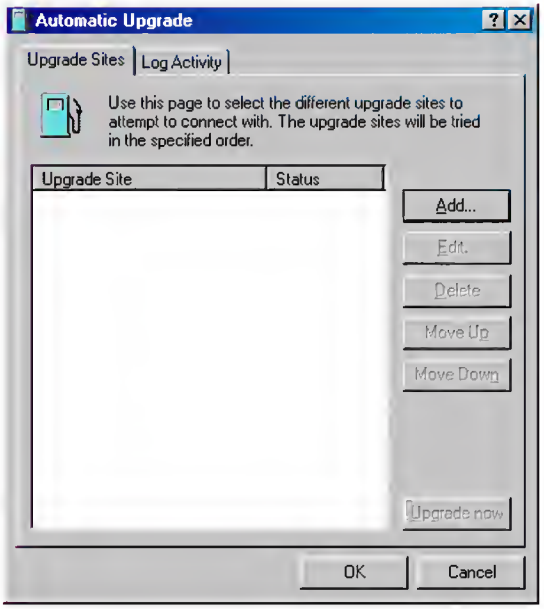

Figure 6-22. Automatic Upgrade dialog box - Upgrade Sites page

Here, AutoUpgrade lists the sites from which it will download new .DAT files. You will not see any sites listed initially, because AutoUpgrade does not come configured to connect to any upgrade site. You must add the sites you need from the information you received when you purchased VirusScan. You can add as many different sites as you need, and alter the order in which AutoUpgrade tries to connect to them, from this dialog box. Your options are:

- **Add a new site.** Click **Add** to open the Automatic Upgrade Properties dialog box (Figure 6-23). To learn how to specify options for your new site, see "Configuring upgrade options" on page 211.

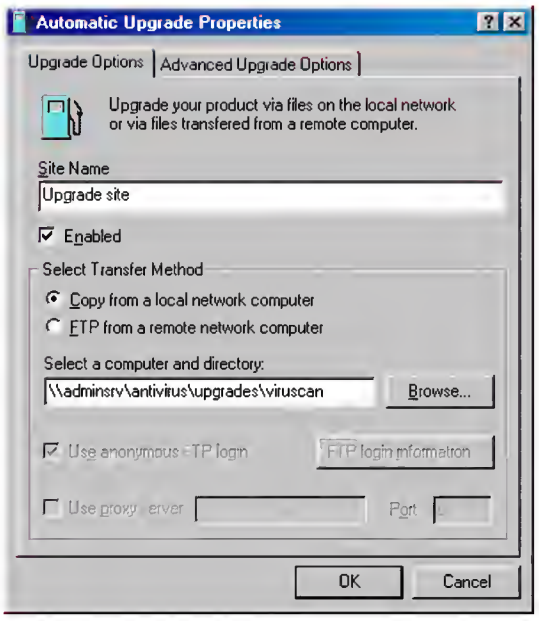

Figure 6-23. Automatic Upgrade Properties dialog box - Upgrade Options page

- **Change the options for an existing site.** Select one of the sites shown in the list, then click **Edit** to open the Automatic Upgrade Properties dialog box (see Figure 6-23 on page 209). Make the changes you want to make, then click **OK** to close the dialog box. To see descriptions and instructions for configuring the available options, see "Configuring upgrade options" on page 211.
- **Remove an existing site.** Select one of the sites shown in the list, then click **Delete** to remove it.
- **Change the search order for existing sites.** To change the order in which AutoUpgrade connects to each site, select the site whose priority you want to change, then click **Move Up** to give the site a higher priority, or **Move Down** to give it a lower priority.
- **Upgrade your VirusScan files immediately.** Click **Upgrade Now** to have AutoUpgrade connect immediately to the first site listed and check for a new VirusScan version. To use this function, you must have configured enough of the necessary options for AutoUpgrade to locate the listed site and, if necessary, log on to it. See "Configuring upgrade options" on page 211 to learn how to specify the options you need.

If AutoUpgrade cannot connect to the listed site after three attempts, or if it does not find new VirusScan files, it will connect to each of the other sites listed until it finds the most current VirusScan version available.

2. Click the Log Activity tab to display the next property page (Figure 6-24).

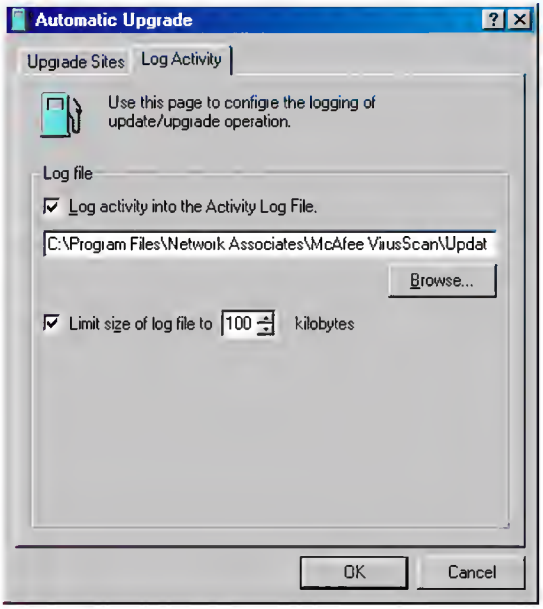

Figure 6-24. Automatic Upgrade dialog box - Log Activity page

3. Select the **Log activity into the Activity Log File** checkbox.

   By default, AutoUpgrade records what happens during update attempts and saves the record in the file UPDATE UPGRADE ACTIVITY LOG.TXT in the VirusScan program directory. You can enter a different name and path in the text box provided, or click **Browse** to locate a suitable file elsewhere on your hard disk or on your network.

4. To minimize the log file size, select the **Limit size of log file to** checkbox, then enter a value for the file size, in kilobytes, in the text box provided.

   Enter a value between 10KB and 999KB. By default, AutoUpgrade limits the file size to 100KB. If the data in the log exceeds the file size you set, AutoUpgrade erases the existing log and begins again from the point at which it left off. To see the contents of the log file from VirusScan Scheduler, select the AutoUpgrade task in the task list, then choose **View Activity Log** from the **Task** menu.

5. Click **OK** to save your changes and close the Automatic Upgrade dialog box. Click **Cancel** to close the dialog box without saving your changes. AutoUpgrade saves all of the changes you make in the Automatic Upgrade dialog box to UPGRADE.INI, a file stored in the VirusScan program directory. To replicate these same settings across your network, copy UPGRADE.INI to the VirusScan program directory on each network node.

Configuring upgrade options

To create a new upgrade site or change the settings for an existing site, click **Add** in the Automatic Upgrade dialog box (see Figure 6-22 on page 208), or select a listed site, then click **Edit**. Either action will open the Automatic Upgrade Properties dialog box (Figure 6-25).

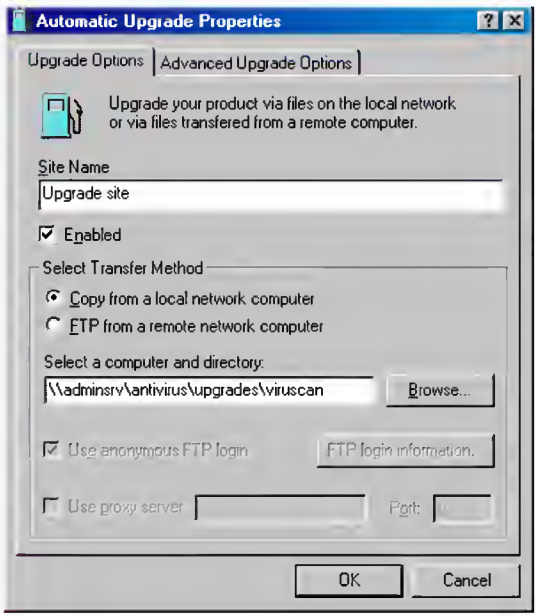

Figure 6-25. Automatic Upgrade Properties dialog box - Upgrade Options page

Next, follow these steps:

1. Type a name for the site in the text box provided. Choose a descriptive name that you will recognize in the site list.
2. Click **Enabled** to tell AutoUpgrade to connect to this site at the time you have scheduled. Clearing the checkbox preserves the options you have configured, but tells AutoUpgrade not to check the site.

   AutoUpgrade will make a maximum of three connection attempts for the site during each scheduled update operation. When it does connect and download a new VirusScan version, AutoUpgrade also extracts the files and installs them into the VirusScan program directory.
3. Choose the method you want to use to connect to the target server. Your choices are:

   - **Copy from a local network computer**. Select this option to simply transfer the update files from a computer somewhere on your network via whichever common network protocol you have active. The settings for this protocol will govern how AutoUpgrade attempts the connection and the length of the timeout period that must pass before AutoUpgrade stops the connection attempt.

     Enter the computer name in Universal Naming Convention (UNC) notation in the text box provided, or click **Browse** to locate the computer on your network. The remaining options in the dialog box become unavailable.

   - **FTP from a remote network computer**. Select this option to transfer the update files via File Transfer Protocol (FTP). To use this option, the target server must have an FTP service enabled.

     AutoUpgrade uses its own FTP implementation to connect to the server, but the timeout period for the connection attempt will depend on your existing network protocol settings.

     Next, enter in the text box provided the domain name for the target server, together with any other necessary directory information, or click **Browse** to locate the server on your network.

     If the target server accepts anonymous FTP logins, select the **Use anonymous FTP login** checkbox. If you use a specific FTP account that requires a user name and password, clear the checkbox, then click **FTP login information** instead. This button opens a dialog box where you can enter the correct user name and password. Enter the password again to confirm it, then click **OK** to close the dialog box.

4. If you route FTP requests through a proxy server, select the **Use proxy server** checkbox, then enter the name of your proxy server in the text box provided. You can enter the name in UNC notation or as a domain name, whichever is appropriate for your environment. Next, in the remaining text box, enter the logical port for the proxy server that AutoUpgrade should address with its FTP request.

5. To choose additional options, click the Advanced Upgrade tab. To save your changes and return to the Automatic Upgrade dialog box, click **OK**. AutoUpgrade saves all of the changes you make in the Automatic Upgrade dialog box to UPGRADE.INI, a file stored in the VirusScan program directory. To close the dialog box without saving your changes, click **Cancel**.

Configuring advanced upgrade options

To complete your AutoUpgrade task, you need to enter only a target server, a connection method, and any necessary login information. Then, once you enable the task and set a schedule for it, AutoUpgrade will download the correct files from the target server for you, extract them, and install them into the VirusScan program directory.

To have AutoUpgrade take other actions before or after it locates new files, click the Advanced Upgrade Options tab to display the correct property page (Figure 6-26).

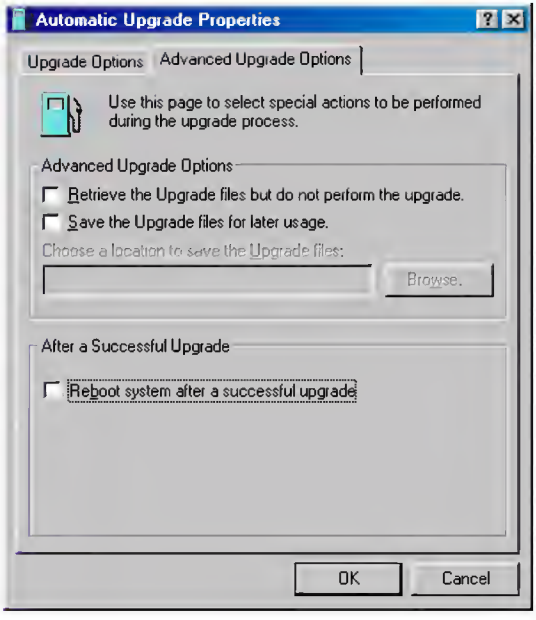
Automatic Upgrade Properties
Upgrade Options
Advanced Upgrade Options
Use this page to select special actions to be performed during the upgrade process.
Advanced Upgrade Options
Retrieve the Upgrade files but do not perform the upgrade.
Save the Upgrade files for later usage.
Choose a location to save the Upgrade files:
Browse...
After a Successful Upgrade
Reboot system after a successful upgrade
OK
Cancel

Figure 6-26. Automatic Upgrade Properties dialog box - Advanced Upgrade Options page

Next, follow these steps:

1. Tell AutoUpgrade what you want it to do with the files it downloads. Your options are:

   - **Retrieve the Upgrade files but do not perform the upgrade**. Select this checkbox to have AutoUpgrade download the new VirusScan version and simply save it in a location you specify instead of installing it.

     Selecting this checkbox also selects the **Save the Update file for later usage** checkbox. To tell AutoUpgrade where to save the new files, enter a path and folder name in the text box below this checkbox, or click **Browse** to locate a suitable folder.

     You might want to use this option if you download new VirusScan files to a central server on your network and want individual client computers to download and install the new files locally.

   - **Save the Upgrade files for later usage.** Select this checkbox to have AutoUpgrade save an unextracted copy of the new VirusScan files in a location you specify. AutoUpgrade then continues with the installation. By contrast, the **Retrieve the Upgrade files but do not perform the update** option saves the unextracted file, but does not install the new VirusScan version.

2. Tell AutoUpgrade what you want it to do after it successfully downloads and installs a new VirusScan version. Your options are:

   - **Reboot system after a successful upgrade**. Select this checkbox to have AutoUpgrade restart your system after it installs new VirusScan files.

     Although VirusScan and VShield need you to restart your system after installation, you might want to do so only during idle hours so as not to interfere with productive work.

     NOTE: This option functions only for scheduled upgrade operations. If you click **Upgrade Now** in the Automatic Upgrade dialog box, AutoUpgrade will ask you if you want to restart your computer as soon as it finishes installing the new VirusScan version , whether you selected this option or not.

     ---

3. To save your changes and return to the Automatic Upgrade dialog box, click **OK**. AutoUpgrade saves all of the changes you make in the Automatic Upgrade dialog box to UPGRADE.INI, a file stored in the VirusScan program directory. To close the dialog box without saving your changes, click **Cancel**.

Configuring options for other programs

You can use the Scheduler to run other programs at specific times, but unless the program you want to run is a Network Associates anti-virus product, you cannot use the Scheduler to configure the program to run with particular options. To do that, you must open and pre-configure the program yourself—the Scheduler will simply run the program as you have it configured at the time you specify. You can, however, use the Scheduler to open the VShield Properties dialog box so that you can configure VShield to run with particular scan options. To learn how to do this, see Chapter 4, "Using VShield."

Using Specialized Scanning Tools 7

Scanning Microsoft Exchange and Outlook mail

In addition to the continuous background scanning that VShield provides you with through its E-Mail Scan module, VirusScan includes a full-featured program component designed specifically to look for viruses in your Microsoft Exchange and Microsoft Outlook mailboxes, or on any mail server that works with Microsoft's Messaging Application Programming Interface (MAPI). The E-Mail Scan program component gives you the ability to scan your mail servers at your own initiative, and at times convenient for you. An unobtrusive plug-in architecture gives you access to the scanner from directly within your Exchange or Outlook client application.

If you installed VirusScan with the Typical installation option (see page 38 for details), you already have access to the E-Mail Scan program component.

To use the E-Mail Scan program component with its default settings, simply start your Microsoft Exchange or Microsoft Outlook client software, then

1. Log on to your mail server as you would normally.
2. Choose **Scan for Viruses** from the **Tools** menu, or click in the Exchange or Outlook toolbar.

> **NOTE:** If you use Microsoft Exchange 5.0, a limitation in the way the program updates its toolbar prevents E-Mail Scan from displaying its buttons immediately. To add the Scan for Viruses button to the toolbar, choose **Customize Toolbar** from the **Tools** menu, then add the E-mail Scan buttons from the list of available buttons in the Customize Toolbar dialog box.

Once you've started it, E-Mail Scan will immediately beginning scanning your Exchange or Outlook mailbox for viruses (see Figure 7-1 on page 218).

By default, E-Mail Scan examines *all* of the mail messages stored in your Inbox on the mail server, looking for attachments susceptible to virus infection. If you have a large number of messages stored there that you have not yet downloaded, this scan operation can take a long time. To pause the operation, click . To stop it altogether, click . To resume the operation, click .

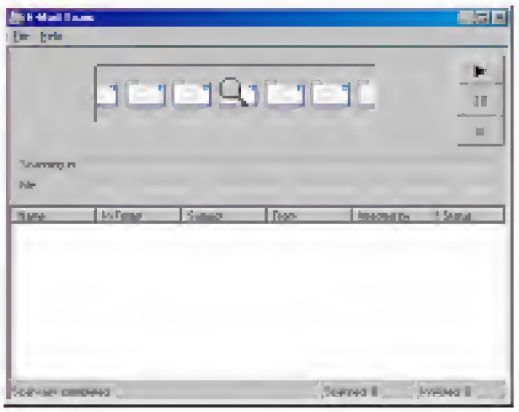

Figure 7-1. E-Mail Scan in progress

If it finds an infected file, E-Mail Scan will ask you how to respond to the virus. See "Responding when E-Mail Scan detects a virus" on page 68 for details.

Configuring the E-Mail Scan program component

Although E-Mail Scan's default settings give you good protection against infections spread via your Exchange or Outlook e-mail, those settings might not suit your work habits.

To modify E-Mail Scan's configuration options, follow these steps:

1. Start your Exchange or Outlook client software, then log onto your e-mail server.

   NOTE: If you have already logged into the network domain that hosts your e-mail server, you might not need to log into to your e-mail server directly—instead, you can simply start Exchange or Outlook. See your network administrator to learn the login requirements for your server.

2. Choose **E-Mail Scan Properties** from the **Tools** menu in either program, or click in the Exchange or Outlook toolbar.

   The E-Mail Scan Properties dialog box will appear (see Figure 7-2 on page 219). The Properties dialog box consists of property pages that control E-Mail Scan's settings—click each tab to set up the program for your needs.

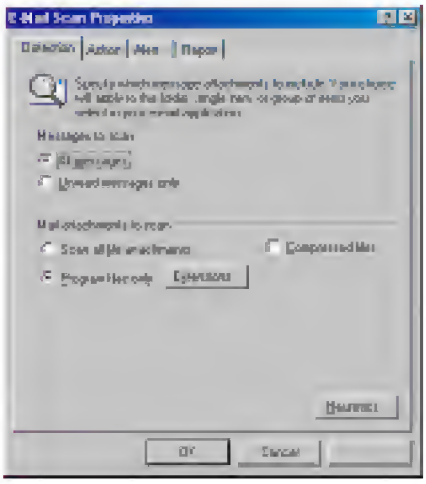

Figure 7-2. E-Mail Scan Properties dialog box - Detection page

Choosing Detection options

E-Mail Scan initially assumes that you want to scan all e-mail messages stored on your Exchange or Outlook server, and to restrict the files it scans only to those susceptible to virus infection (see Figure 7-2).

To change these settings, follow these steps:

1. Tell E-Mail Scan which e-mail messages you want it to scan. Your choices are:

   - **All messages.** Select this button to have E-Mail Scan look at all messages now stored on your Exchange server. This scan, while thorough, can take a long time.
   - **Unread messages only.** Select this button to have E-Mail Scan examine only those messages marked "unread." After you scan your entire mailbox, choose this option to speed up scan operations, while maintaining complete anti-virus protection for your computer.

     NOTE: Once you download mail to your computer, VirusScan treats your personal folder or archive file as it would any other file, unless you specifically exclude it from scanning operations. This gives you an added layer of anti-virus security.

2. Tell E-Mail Scan which types of attachments you want it to examine. You can

   - **Scan compressed files.** Select the **Compressed files** checkbox to have E-Mail Scan look for viruses in files compressed with these formats: .??_, .CAB, LZEXE, LZH, PKLite, .TD0, and .ZIP. Although it does give you better protection, scanning compressed files can lengthen a scan operation.

   - **Choose file types for scanning.** Viruses ordinarily cannot infect data files or files that contain no executable code. You can, therefore, safely narrow the scope of your scan operations so that E-Mail Scan looks only at those attachments most susceptible to virus infection. To do so, select the **Program files only** button. To see or designate the file name extensions E-Mail Scan will examine, click **Extensions** to open the Program File Extensions dialog box (Figure 7-3).

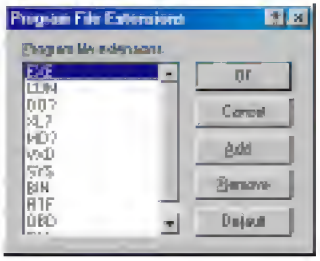

Figure 7-3. Program File Extensions dialog box

By default, E-Mail Scan looks for viruses in files with the extensions .EXE, .COM, .DO?, .XL?, .RTF, .BIN, .SYS, .MD?, .VXD, .OBD, and .DLL. Files with .DO?, .XL?, .RTF, and .OBD extensions are Microsoft Office files, all of which can harbor macro virus infections. The ? character is a wildcard that enables E-Mail Scan to scan document and template files.

   - To add to the list, click **Add**, then type the extensions you want E-Mail Scan to scan in the dialog box that appears.
   - To remove an extension from the list, select it, then click **Remove**.
   - Click **Default** to restore the list to its original form.

When you have finished, click **OK** to close the dialog box.

To have E-Mail Scan examine all files on your system, whatever their extensions, select the **Scan all file attachments** button. This will slow your scan operations down considerably, but will ensure that your system is virus free.

- **Turn on heuristic scanning**. Click **Heuristics** to open the Heuristics Scan Settings dialog box (Figure 7-4).

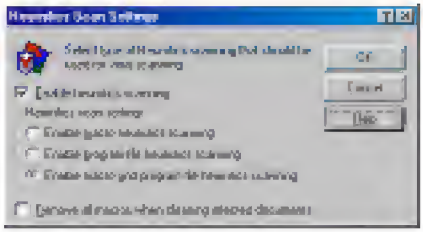

Figure 7-4. Heuristics Scan Settings dialog box

Heuristic scan technology enables E-Mail Scan to recognize new viruses based on their resemblance to similar viruses VirusScan already knows. To do this, the program looks for "virus-like" characteristics in the files you've asked it to scan. The presence of a sufficient number of these characteristics in a file leads E-Mail Scan to identify the file as potentially infected with a new or previously unidentified virus.

Because E-Mail Scan looks simultaneously for file characteristics that rule out the possibility of virus infection, it will rarely give you a false indication of a virus infection. Therefore, unless you know that the file does *not* contain a virus, you should treat "potential" infections with the same caution you would confirmed infections.

To activate heuristic scanning, follow these steps:

a. Select the **Enable heuristics scanning** checkbox. The remaining options in the dialog box activate.

b. Select the types of heuristic scanning you want E-Mail Scan to use. Your choices are:

- **Enable macro heuristics scanning**. Choose this option to have E-Mail Scan identify all Microsoft Word, Microsoft Excel, and other Microsoft Office files that have embedded macros, then compare the macro code to its virus signature database. E-Mail Scan will identify exact matches with the virus name; code signatures that resemble existing viruses cause E-Mail Scan to tell you it has found a potential macro virus.
- **Enable program file heuristics scanning.** Choose this option to have E-Mail Scan locate new viruses in program files by examining their characteristics and comparing them against a list of known virus characteristics. E-Mail Scan will identify files with a sufficient number of these characteristics as potential viruses.

- **Enable macro and program file heuristics scanning.** Choose this option to have E-Mail Scan use both types of heuristic scanning. Network Associates recommends that you use this option for complete anti-virus protection.

c. Determine how you want to treat infected macro files. Select **Remove all macros when cleaning infected documents** to eliminate all infectable code from the document and leave only data. To try to remove only the virus code from the document's macros, leave this checkbox clear.

> **WARNING:** Use this feature with caution: removing all macros from a document can cause it to lose data or to become corrupted and unusable.

d. Click **OK** to save your settings and return to the E-Mail Scan Properties dialog box.

3. Click the Action tab to choose additional E-Mail Scan options. To save your changes without closing the E-Mail Scan Properties dialog box, click **Apply**. To save your changes and close the dialog box, click **OK**. To close the dialog box without saving your changes, click **Cancel**.

> **NOTE:** Clicking **Cancel** will not undo any changes you already saved by clicking **Apply**.

Choosing Action options

When E-Mail Scan detects a virus, it can respond either by asking you what it should do with the infected file, or by automatically taking an action that you determine ahead of time. Use the Action property page to specify which response options you want E-Mail Scan to give you when it finds a virus, or which actions you want it to take on its own.

Follow these steps:

1. Click the Action tab in the E-Mail Scan Properties dialog box to display the correct property page (Figure 7-5).

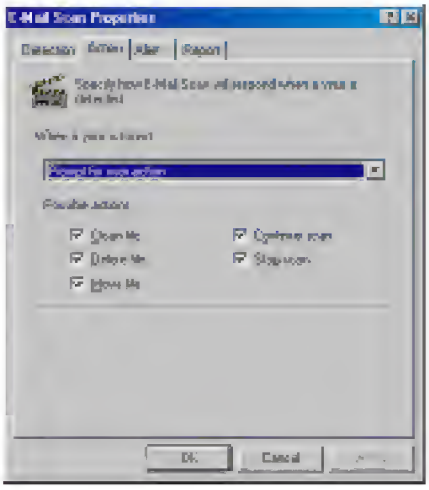

Figure 7-5. E-Mail Scan Properties dialog box - Action page

2. Choose a response from the **When a virus is found** list. The area immediately beneath the list will change to show you additional options for each choice. Your choices are:

   - **Prompt for user action.** Use this option if you expect to be at your computer when E-Mail Scan examines your disk—the program will display an alert message when it finds a virus and offer you a range of possible responses. Select the response options you want to see in the alert message:
     - **Clean file.** This option tells E-Mail Scan to try to remove the virus code from the infected file.
     - **Delete file.** This option tells E-Mail Scan to delete the infected file immediately.
     - **Move file.** This option tells E-Mail Scan to move the infected file to a quarantine folder.
     - **Continue scan.** This option tells E-Mail Scan to continue with its scan, but not take any other actions. If you have its reporting options enabled, E-Mail Scan records the incident in its log file.
     - **Stop scan.** This option tells E-Mail Scan to stop the scan operation immediately. To continue, you must click **Scan Now** to restart the operation.

- **Move infected attachment automatically**. Use this option to have E-Mail Scan move infected files to a quarantine directory named INFECTED. E-Mail Scan will create the INFECTED folder on the Exchange or Outlook mail server.

  You cannot designate a different folder or change the folder's name, but the INFECTED folder will appear under your mailbox folder. You can open the folder and view the message if you wish, but note that doing so could expose your computer to virus infection.

- **Clean infected attachment automatically.** Use this option to tell E-Mail Scan to remove the virus code from the infected attachment as soon as it finds it. If E-Mail Scan cannot remove the virus, it will notify you in its message area and, if you have its reporting features enabled, will note the incident in its log file. See "Choosing Report options" on page 227 for details.

- **Delete infected attachment automatically.** Use this option to have E-Mail Scan delete every infected attachment it finds immediately. Be sure to enable its reporting feature so that you have a record of which attachments E-Mail Scan deleted. You will need to restore deleted files from backup copies.

  WARNING: E-mail Scan will *not* try to break any encrypted messages to scan them. If an infected attachment includes a digital signature, E-Mail Scan will *remove* the digital signature in order to clean or delete the infected file.

- **Continue scanning.** Use this option only if you plan to leave your computer unattended while E-Mail Scan checks for viruses. If you also activate the E-Mail Scan reporting feature (see "Choosing Report options" on page 227 for details), the program will record the names of any viruses it finds and the names of infected files so that you can delete them at your next opportunity.

3. Click the Alert tab to choose additional E-Mail Scan options. To save your changes without closing the E-Mail Scan Properties dialog box, click **Apply**. To save your changes and close the dialog box, click **OK**. To close the dialog box without saving your changes, click **Cancel**.

   NOTE: Clicking **Cancel** will not undo any changes you already saved by clicking **Apply**.

Choosing Alert options

Once you configure it with the response options you want, you can let E-Mail Scan look for and remove viruses from your system automatically, as it finds them, with almost no further intervention. If, however, you want E-Mail Scan to inform you immediately when it finds a virus so that you can take appropriate action, you can configure it to send an alert message to you in a variety of ways. Use the Alert property page to choose which alerting methods you want to use.

Follow these steps:

1. Click the Alert tab in the E-Mail Scan Properties dialog box to display the correct property page (Figure 7-6).

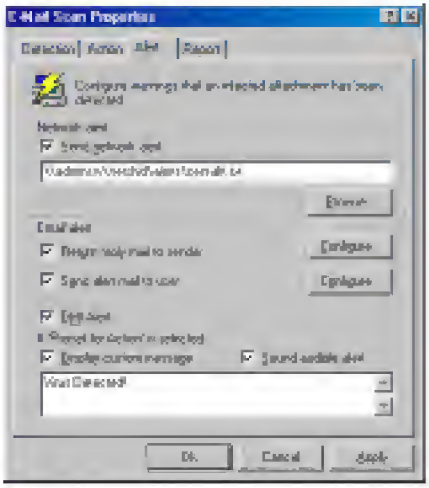

Figure 7-6. E-Mail Scan Properties dialog box - Alert page

2. To tell E-Mail Scan to send an alert message to a server running NetShield, a Network Associates server-based anti-virus solution, select the **Send network alert** checkbox, then enter the path to the NetShield alert folder on your network, or click **Browse** to locate the correct folder.

> **NOTE:** The folder you choose must contain CENTALRT.TXT, the NetShield Centralized Alerting file. NetShield collects alert messages from E-Mail Scan and other Network Associates software, then passes them to network administrators for action. To learn more about Centralized Alerting, see the NetShield *User's Guide*.

3. To send an alert message to the person who sent you the infected e-mail attachment, select the **Return reply mail to sender** checkbox. You can then compose a standard reply to send. Follow these steps:

   a. Click **Configure** to open a standard mail message form.

   b. Fill in the subject line, then add any comments you want to make in the body of the message, below a standard infection notice that E-Mail Scan will supply. You may add up to 1024 characters of text.

   c. To send a copy of this message to someone else, enter an e-mail address in the text box provided, or click **Cc:** to choose a recipient from your mail system's user directory or address book.

   d. Click **OK** to save the message.

   Whenever it detects a virus, E-Mail Scan will send a copy of this message to each person who sends you e-mail with an infected attachment. It fills in the recipient's address with information found in the original message header, and identifies the virus and the affected file in the area immediately below the subject line. If you have activated its report feature, E-Mail Scan also logs each instance when it sends an alert message.

4. To send an e-mail message to warn others about an infected attachment, select the **Send alert mail to user** checkbox. You can then compose a standard reply to send to one or more recipients—a network administrator, for example—each time E-Mail Scan detects an infected e-mail attachment. Follow these steps:

   a. Click **Configure** to open a standard mail message form.

   b. Enter an e-mail address in the text box provided, or click **To:** to choose a recipient from your mail system's user directory or address book. Repeat the process in the text box labeled **Cc:** to send a copy of the message to someone else.

   > **NOTE:** To find an e-mail address in this way, you must have access to a MAPI-compliant user directory. If you are working offline and have not yet logged onto your e-mail system, E-Mail Scan asks you to choose a user profile it can use to log onto your system. Enter the requested information, then click **OK** to continue.

   c. Fill in the subject line, then add any comments you want to make in the body of the message below the infection notice. You may add up to 1024 characters of text.

   d. Click **OK** to save the message.

Whenever it detects a virus, E-Mail Scan sends a copy of this message to each of the addresses that you entered in Step b. It adds information to identify the virus and the affected file in the area immediately below the subject line. If you have activated its report feature, E-Mail Scan also logs each instance when it sends an alert message.

5. To have E-Mail Scan send virus alert messages via the DMI Component Interface to desktop and network management applications running on your network, select the **DMI Alert** checkbox.

> **NOTE:** The Desktop Management Interface is a standard for communicating management requests and alert information between hardware and software components stored on or connected to desktop computers, and the applications used for managing them. To learn more about using this alert method, see your network administrator.

6. If you chose **Prompt for user action** as your response in the Action page (see page 223 for details), you can also tell E-Mail Scan to beep and display a custom message when it finds a virus. To do so, select the **Display custom message** checkbox, then enter the message you want to see in the text box provided—you can enter a message up to 225 characters in length. Next, select the **Sound audible alert** checkbox.

7. Click the Report tab to choose additional E-Mail Scan options. To save your changes without closing the E-Mail Scan Properties dialog box, click **Apply**. To save your changes and close the dialog box, click **OK**. To close the dialog box without saving your changes, click **Cancel**.

> **NOTE:** Clicking **Cancel** will not undo any changes you already saved by clicking **Apply**.

Choosing Report options

E-Mail Scan lists its current settings and summarizes all of the actions it takes during its scanning operations in a log file called MAILSCAN.TXT. You can have E-Mail Scan write its log to this file, or you can use any text editor to create a text file for E-Mail Scan to use. You can then open and print the log file for later review from within E-Mail Scan or from a text editor.

Use the Reports property page to determine which information E-Mail Scan will include in its log file.

To set E-Mail Scan to record its actions in a log file, follow these steps:

1. Click the Report tab in the E-Mail Scan Properties dialog box to display the correct property page (Figure 7-7).

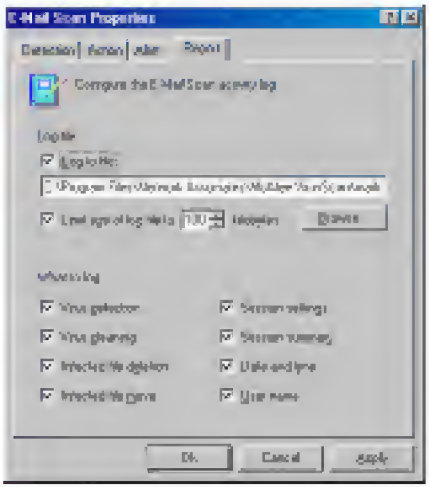

Figure 7-7. E-Mail Scan Properties dialog box - Report page

2. Select the **Log to file** checkbox.

   By default, E-Mail Scan writes log information to the file MAILSCAN.TXT in the VirusScan program directory. You can enter a different name in the text box provided, or click **Browse** to locate a suitable file elsewhere on your hard disk or on your network.

3. To minimize the log file size, select the **Limit size of log file to** checkbox, then enter a value for the file size, in kilobytes, in the text box provided.

   Enter a value between 10KB and 999KB. By default, E-Mail Scan limits the file size to 100KB. If the data in the log exceeds the file size you set, E-Mail Scan erases the existing log and begins again from the point at which it left off.

4. Select the checkboxes that correspond to the information you want E-Mail Scan to record in its log file. You can choose to record any of this information:

   - **Virus detection.** Select this checkbox to have E-Mail Scan note the number of infected files it found during this scanning session.
   - **Virus cleaning.** Select this checkbox to have E-Mail Scan note the number of infected files from which it removed the infecting virus.

- **Infected file deletion.** Select this checkbox to have E-Mail Scan note the number of infected files it deleted from your e-mail server.
- **Infected file move.** Select this checkbox to have E-Mail Scan note the number of infected files it moved to the quarantine directory on your mail server.
- **Session settings.** Select this checkbox to have E-Mail Scan list the options you choose in the E-Mail Scan Properties dialog box for each scanning session.
- **Session summary.** Select this checkbox to have E-Mail Scan summarize its actions during each scanning session. Summary information includes the number of files scanned, the number and type of viruses detected, the number of files moved or deleted, and other information.
- **Date and time.** Select this checkbox to have E-Mail Scan append the date and time to each log entry it records.
- **User name.** Select this checkbox to have E-Mail Scan append the name of the user logged in to your e-mail server at the time it records each log entry.

5. Click a different tab to change any of your E-Mail Scan settings. To save your changes without closing the E-Mail Scan Properties dialog box, click **Apply**. To save your changes and close the dialog box, click **OK**. To close the dialog box without saving your changes, click **Cancel**.

> **NOTE:** Clicking **Cancel** will not undo any changes you already saved by clicking **Apply**.

Scanning cc:Mail

VirusScan includes native support for later-generation e-mail client software based on Microsoft's MAPI standard, including Microsoft's own Exchange and Outlook clients, and version 8.0 and later of Lotus Development's cc:Mail product. If you use earlier cc:Mail versions—v6.0 or v7.0—you will need to install VirusScan's cc:Mail Scan component to have it look for viruses in your Inbox.

> **IMPORTANT:** To install the cc:Mail Scan component, you must choose the Custom installation option during Setup—VirusScan does not install this component by default. See page 38 for details.

Once installed, cc:Mail Scan plugs into VShield, logs on to your cc:Mail system, then operates unobtrusively in the background, polling your cc:Mail Inbox to check for new mail. When new mail arrives, cc:Mail Scan calls VShield to examine it for any infected attachments before your client software downloads it to your computer.

The only real interaction you will have with cc:Mail Scan is when you choose which corporate e-mail system you want VShield to scan for viruses. To learn how to specify cc:Mail as your corporate e-mail system, see Chapter 4, page 97.

If you have not yet logged in to your cc:Mail server, cc:Mail Scan might also ask you to enter your user name and password into a login screen so that VShield can get access to your cc:Mail server and scan your Inbox. Enter your cc:Mail user name and password, just as if you were logging directly into cc:Mail, then click **OK** to continue. Next, start your cc:Mail client application, then set the interval for the client to poll your cc:Mail server to a period longer than five minutes. This gives VShield a chance to examine your mail before your client software retrieves it.

The cc:Mail component logs off from your e-mail server when you quit your client software.

Using ScreenScan

VirusScan's ScreenScan component provides you with background virus scanning as your computer's screen saver runs. With it, you can turn otherwise idle computer time to productive use by allowing your machine to check itself for virus infections. ScreenScan will not take any action against viruses it detects, but it will record the results of its scan operations in a log file that you can review at your leisure.

To use ScreenScan, you must choose the Custom installation option during Setup—VirusScan does not install this component by default. See page 38 for details. Once installed, ScreenScan displays a property page in the Windows Display Properties dialog box. Here you can choose the detection and report options that you want ScreenScan to use.

To configure ScreenScan, follow these steps:

1. Click **Start** in the Windows taskbar, point to **Settings**, then choose **Control Panel**.

2. Locate and double-click the Display control panel in the window that appears in order to open the Display Properties dialog box. Next, click the McAfee ScreenScan tab to display the correct property page (see Figure 7-8 on page 231).

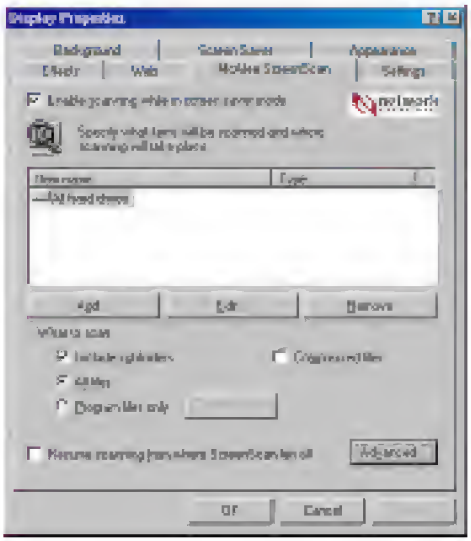

Figure 7-8. Display Properties dialog box - McAfee ScreenScan page

3. Select the **Enable scanning while in screen saver mode** checkbox to activate the options in the rest of the property page.

4. Choose which parts of your system that you want ScreenScan to examine for viruses. You can

   - **Add scan targets.** Click **Add** to open the Add Scan Item dialog box (Figure 7-9).

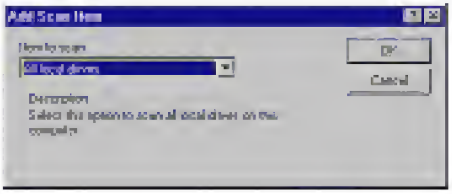

Figure 7-9. The Add Scan Item dialog box

Next, choose the scan target from the list provided. Your choices are:

– **All local drives.** This tells ScreenScan to scan all drives, both hard disks and floppy disks, either physically attached to your computer or inserted in a floppy drive. This is the safest and most comprehensive option available in ScreenScan.

– **All fixed drives.** This tells ScreenScan to scan only hard disks physically connected to your computer.

– **Drive or folder.** This tells ScreenScan to scan a particular disk or folder on your computer. In the text box provided, type the drive letter or the path to the folder you want scanned, or click **Browse** to locate the scan target on your computer. Click **OK** to close the dialog box.

> **IMPORTANT:** To scan all of the subfolders in your scan target, be sure to select the **Include subfolders** checkbox in the **What to Scan** area in the ScreenScan property page.

- **Change scan targets.** Select one of the listed scan targets, then click **Edit** to open the Edit Scan Item dialog box (Figure 7-10).

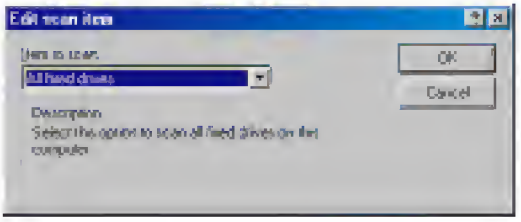

Figure 7-10. The Edit Scan Item dialog box

The dialog box appears with the existing scan target specified. Choose or enter a new scan target, then click **OK** to close the dialog box.

- **Remove scan targets.** Select one of the listed scan targets, then click **Remove** to delete it.

5. Specify the types of files you want ScreenScan to examine. You can

   - **Scan compressed files.** Select the **Compressed files** checkbox to have ScreenScan look for viruses in files compressed in .CAB, LZH, or .ZIP archiving formats.

   - **Choose file types for scanning.** Viruses ordinarily cannot infect data files or files that contain no executable code. You can, therefore, safely narrow the scope of your scan operations so that ScreenScan looks only at those attachments most susceptible to virus infection. To do so, select the **Program files only** button. To see or designate the file name extensions ScreenScan will examine, click **Extensions** to open the Program File Extensions dialog box (see Figure 7-11 on page 233).

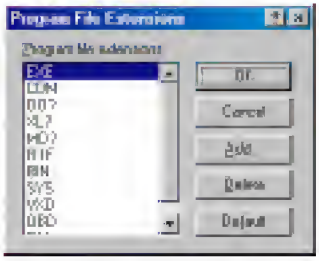

Figure 7-11. The Program File Extensions dialog box

By default, ScreenScan looks for viruses in files with the extensions .EXE, .COM, .DO?, .XL?, .MD?, .RTF, .BIN, .SYS, .VXD, .OBD, and .DLL. Files with .DO?, .XL?, .RTF, and .OBD extensions are Microsoft Office files, all of which can harbor macro virus infections. The ? character is a wildcard that enables ScreenScan to scan document and template files.

- To add to the list, click **Add**, then type the extensions you want ScreenScan to scan in the dialog box that appears.
- To remove an extension from the list, select it, then click **Delete**.
- Click **Default** to restore the list to its original form.

When you have finished, click **OK** to close the dialog box.

To have ScreenScan examine all files on your system, whatever their extensions, select the **All files** button. This will slow your scan operations down considerably, but will ensure that your system is virus free.

6. Determine how you want ScreenScan to balance its scan operations against other work priorities for your computer. Click **Advanced** to open the Advanced Scanner Settings dialog box (Figure 7-12).

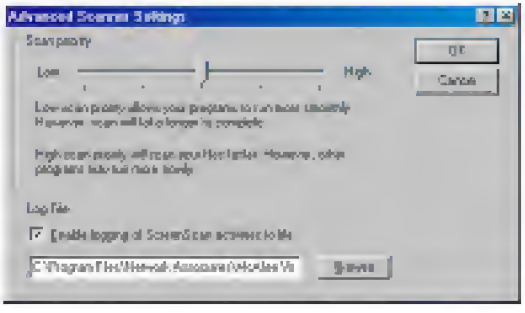

Figure 7-12. Advanced Scanner Settings dialog box

Drag the slider to the left to give ScreenScan a lower priority relative to other programs running on your computer—including your screen saver. This causes ScreenScan to take longer to scan your system, but allows your other programs to run smoothly. Drag the slider to the right to give ScreenScan a relatively high priority for its scanning tasks. It will complete its scan operation more quickly, but other programs running at the same time will not run as smoothly.

7. Enable ScreenScan's report feature.

   Select the **Enable logging of ScreenScan activities to file** checkbox. By default, ScreenScan records its actions in a text file named SCREENSCAN ACTIVITY LOG.TXT. To choose a different text file to use as ScreenScan's report file, enter its path and file name in the text box provided, or click **Browse** to locate a suitable file on your hard disk.

   > **NOTE:** ScreenScan does not create new report files. To have the program use a different log file, you must choose an existing text file that ScreenScan can open and write to.

   Click **OK** to save your changes and close the dialog box. To close the dialog box without saving your changes, click **Cancel**.

8. To have ScreenScan start scanning from the point at which it left off when interrupted, select the **Resume Scanning where ScreenScan left off** checkbox. If you do not select this checkbox, ScreenScan will begin its scan operation with the first item listed in your chosen scan target, whether or not it has already completed a scan operation on that target.

9. Click **Apply** to save your changes without closing the Display Properties dialog box. To save your changes and close the dialog box, click **OK**. To close the dialog box without saving your changes, click **Cancel**.

   > **NOTE:** Clicking **Cancel** will not undo any changes you already saved by clicking **Apply.**

ScreenScan will run the next time your current screen saver does. If you change screen savers, you should reconfigure your ScreenScan options also.

Using SecureCast to Update Your Software A

Introducing SecureCast

The Network Associates SecureCast service conveniently delivers the latest product and data file updates to your desktop. With it, you can choose to receive updates for your licensed Network Associates software via the Internet, regularly and automatically. To use this option, you must install the SecureCast client software and subscribe to either the Home SecureCast channel (for retail customers) or the Enterprise SecureCast channel (for corporate customers).

If you are a retail customer and would rather decide when to update your system, an option allows you to download new files only when your software reminds you that it's time to update. If you are a corporate customer (but not an administrator), contact your administrator to learn where to update your files, or use the AutoUpdate feature if your product includes it.

Choose one of the update options listed in this appendix to keep your system efficiently protected from the network to the desktop. With SecureCast, you'll get the latest data files and program files as soon as they're available. New viruses and other harmful agents appear at a rate of more than 200 per month—don't risk letting your data disintegrate or your network become inaccessible simply because you forgot to update or upgrade your software.

❑ **NOTE:** The term "update" means integrating your product with new versions of data (.DAT) files; the term "upgrade" refers to product version revisions, executables, and data files. Network Associates offers free .DAT file updates for the life of your product. This does not, however, guarantee that .DAT files will be compatible with previous product versions. By upgrading your software to the latest product version and updating to the latest .DAT files regularly via SecureCast, you ensure complete protection for the term of your software subscription or maintenance plan.

Why would I need to update my data files?

To offer you the best protection possible, Network Associates continually updates data files that detect new viruses and other harmful agents. Although your software has technology that allows it to detect previously unknown strains of viruses or malicious code, new virus types and other agents appear frequently. Often, your existing software cannot detect these intruders because the data files that came with it became outdated. Your software periodically notifies you to update these files. For maximum protection, Network Associates strongly recommends that you update your files on a regular basis.

Which data files does SecureCast deliver?

With SecureCast, you'll receive automatic downloads of these common data files:

- NAMES.DAT—includes virus names and other details that the user sees when viewing the Virus List.
- SCAN.DAT—includes detection string data for all viruses detected.
- CLEAN.DAT—includes removal string data for all viruses cleaned.

In addition to the common .DAT files above, you may also receive some of these additional files, depending on which anti-virus or security products you're running:

- WEBSCANX.DAT or INTERNET.DAT—includes detection string data for hostile Java applets and ActiveX controls. WebShieldX and VirusScan use these files.
- MCALYZE.DAT—includes detection string data for complex polymorphic virus detection. Network Associates 32-bit products with engine versions 3.0.0 through 3.1.4 use this file.
- POLYSCAN.DAT—includes detection string data for complex polymorphic virus detection. Network Associates 32-bit products with engine versions 3.1.5 and later use this file.

System requirements

- Windows 95 or later, or Windows NT
- At least 100MB free hard disk space: Home SecureCast (client and channel) 7MB, plus 3–6MB per download. Enterprise SecureCast (client and channel) 15MB, plus 6–6.5MB per download.
- An active Internet connection—direct or dial-up—for a minimum of one hour per week.

SecureCast features

- SecureCast uses client software developed with BackWeb Technologies.
- SecureCast eliminates the need for downloading update files from Network Associates electronic services.
- SecureCast works invisibly in the background, allowing other applications to take priority over it and using your Internet connection when it's idle. You can also configure your desktop client so that SecureCast downloads have a higher priority.
- SecureCast works with most corporate firewalls.
- SecureCast supports 32-bit TCP/IP connections for Enterprise SecureCast and Home SecureCast channel subscribers, and provides non-Internet connections for retail customers using asynchronous modem dialup.
- SecureCast delivers .ZIP, .EXE, and .DAT files to your desktop as BackWeb InfoPaks.

Free services

- Automatic delivery of .DAT files. New .DAT files are usually available mid-month.
- Alerts on newly identified dangerous viruses.
- Announcements of new versions of software and associated products.

Home SecureCast Channel

Retail customers may install SecureCast client software from a Network Associates CD-ROM.

Understanding SecureCast

If you are a retail customer, you can use SecureCast's timely, free delivery service in one of two ways:

- To receive automatic downloads of the latest updates for your licensed Network Associates software via the Internet, install the SecureCast client, then subscribe to the Home SecureCast channel; or
- If you would rather decide when to update your software, use the included update utility when your software reminds you that it's time.

Downloading automatically

Setting up Home SecureCast

To subscribe to the Home SecureCast channel, follow these steps:

1. Install the BackWeb client software from a Network Associates CD-ROM.

   You will receive a Welcome InfoPak that tells you that your connection to the Home SecureCast channel is working. An InfoPak can contain sounds, animations, Web pages, and more. When you receive a new InfoPak from Home SecureCast, it will automatically appear as an animated object on your desktop until you open it. To open an InfoPak, simply double-click it.

2. Complete the channel registration process via the User Registration Information dialog box (which will appear in either the first or second InfoPak you receive), then click **Next**.

   The Online Activity Status dialog box tracks the status of your data transmission.

3. When your user registration is complete, make a note of your registration number, then click **Finish**.

Using Home SecureCast

You are now ready to receive periodic Virus Alerts, plus product updates and upgrades. Within a few days, you should receive additional InfoPaks. Double-click these to extract and set up the updates or upgrades they contain.

Unsubscribing from Home SecureCast

To cancel this service at any time, follow these steps:

1. Double-click the SecureCast client icon in the Windows taskbar status area.
2. Right-click the **Home** channel button.

   A shortcut menu appears.

3. Click **Unsubscribe**, then click **OK** to confirm.

Initiating a Download

Updating registered software

Network Associates software includes a feature that periodically reminds you to update your software. If many months have passed since you first installed your software, Network Associates strongly recommends that you use the update options described in the following sections to ensure that you are using the latest data files and product versions available.

Updating after installation

After you install your anti-virus or security software, the Welcome dialog box (Figure A-1) prompts you to update your software. This dialog box also appears when you start a computer system pre-loaded with Network Associates software for the fifth time. McAfee VirusScan, for example, displays this notice:

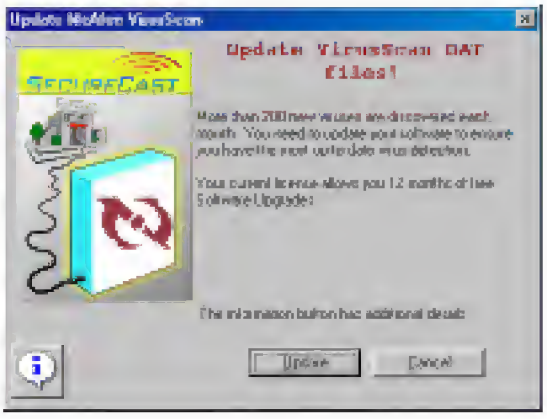

Figure A-1. Welcome dialog box

1. Click **Update** to receive the latest version of the software for free.

The Internet Access dialog box (Figure A-2) appears.

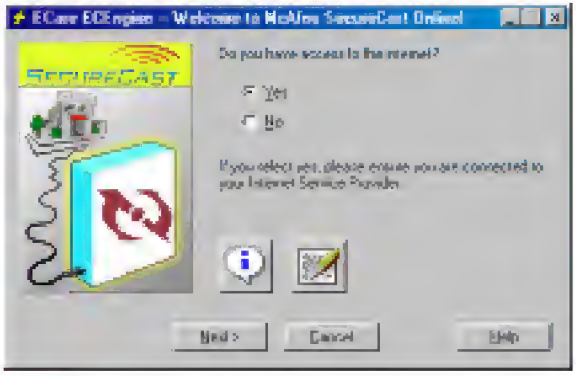

Figure A-2. Internet Access dialog box

2. If you have Internet access, select **Yes**, then click **Next**. If you do not have Internet access, select **No**, then click **Next**.

   - If you selected **Yes**, the User Registration dialog box appears (Figure A-4).

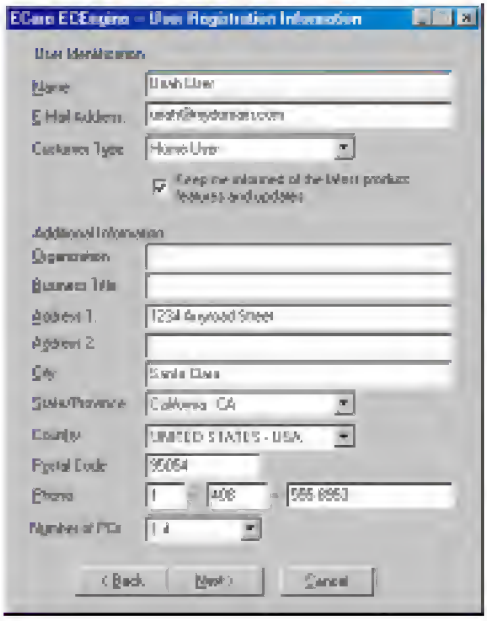

Figure A-3. User Registration dialog box

Fill in the information requested. To move between each text box, press TAB on your keyboard. When you have finished, click **Next>**.

- If you selected **No**, the download server dialog box will appear (Figure A-4). Here, you need to enter or verify your country code and area code, then choose the dial-up server closest to your location.

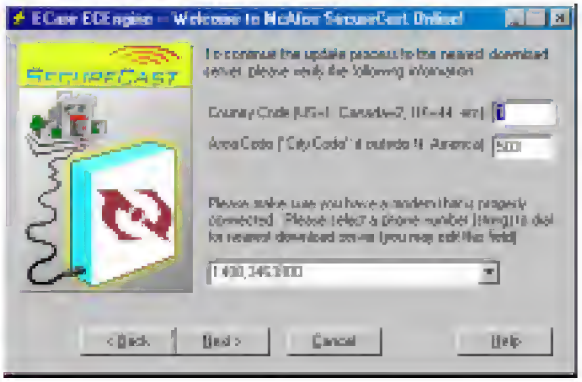

Figure A-4. Server dialog box

NOTE: Downloading .DAT files from Network Associates dial-up servers might cause you to incur long-distance charges.

When you have finished, click **Next>** to continue.

Your system connects to a Network Associates server.

- If the server has no new .DAT file updates or software upgrades, the Online Activity Status dialog box (Figure A-5) tells you that your files are up-to-date.

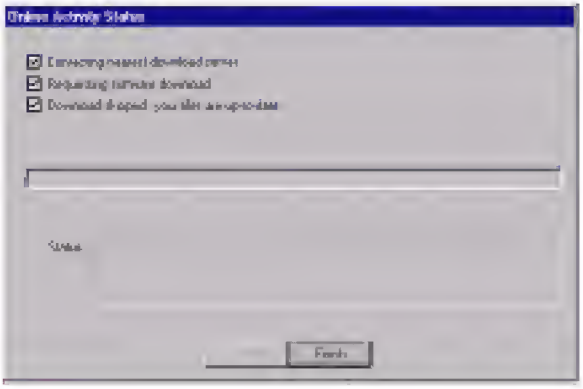

Figure A-5. Online Activity Status dialog box (No Download)

Click **Finish** to disconnect from the server.

- If the server has new .DAT files, the Online Activity Status dialog box (Figure A-6) tells you that the .EXE file containing the .DAT files is automatically downloading to your system.

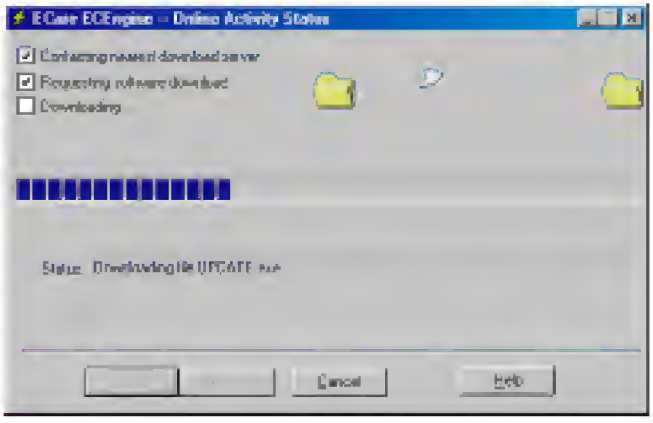

Figure A-6. Online Activity Status dialog box

a. When the download is complete, click **Next**. The Online Activity Complete dialog box (Figure A-7) appears.

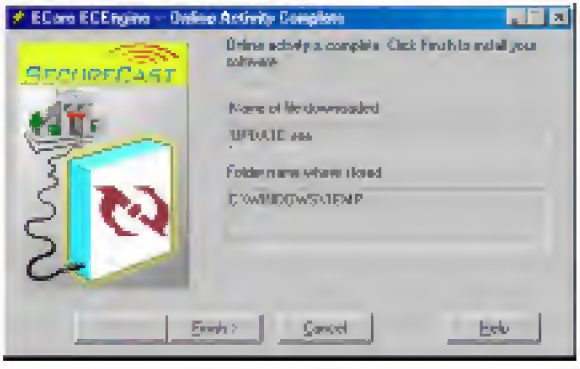

Figure A-7. Online Activity Complete dialog box

b. Click **Finish** to install your new .DAT file updates.

- If the server has a product version more recent than yours, the Newer Component Found dialog box (Figure A-8) appears. To download only the latest .DAT files, select **DAT files only**, then click **Next**. To download a new product version, click **Next**.

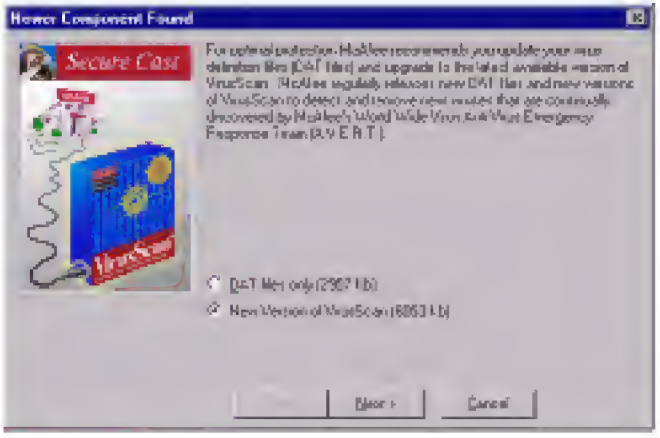

Figure A-8. Newer Component Found dialog box

The Online Activity Status dialog box (see Figure A-6 on page 242) tracks the status of your download. When your download is complete, click **Next** to continue.

The Online Activity Complete dialog box (Figure A-9) confirms that your download is complete.

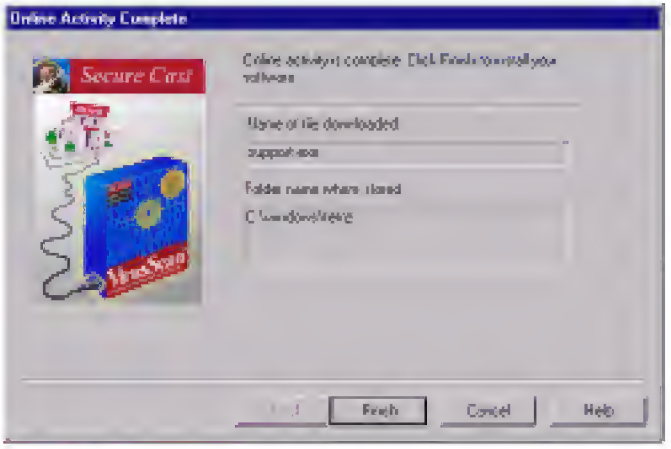

Figure A-9. Online Activity Complete dialog box

3. Note the name and location of the downloaded file, then click **Finish** to install your software.

Updating at periodic intervals

At 30-day intervals, the Update dialog box (Figure A-10) prompts you to update your software.

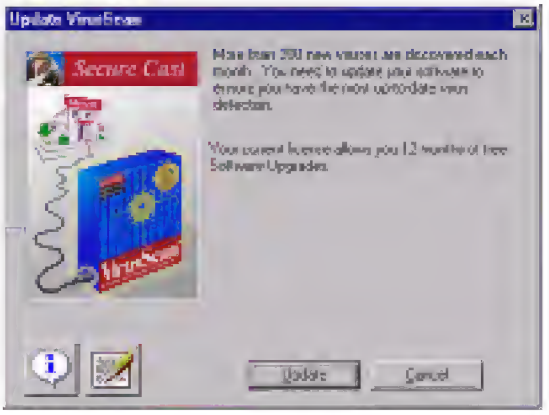

Figure A-10. Update dialog box

If you are a registered user, complete the following steps to receive the latest data file versions free. Repeat these steps every month when your software suggests that you do in order to keep your product updated.

NOTE: As a registered user, you can continue to receive .DAT file updates for the life of your product. Network Associates cannot, however, guarantee compatibility between future .DAT file updates and older product versions. By purchasing the latest software upgrades via SecureCast, you ensure complete virus protection for the term of your software subscription or maintenance plan.

1. Click **Update** to receive the latest data file version for free.

   The Internet Access dialog box (see Figure A-2 on page 240) appears.

2. If you have Internet access, select **Yes**, then click **Next**. If you do not have Internet access, select **No**, then click **Next**.

   The Server dialog box (see Figure A-4 on page 241) appears. If you selected **Yes**, then the dialup-number box will be unavailable; if you selected **No**, then the dialup-number box will be available.

3. If you have Internet access, verify your Country Code and Area Code, then click **Next**. If you don't have Internet access, verify your Country Code and Area Code, select a modem dialup number, then click **Next**.

   Your system connects to a Network Associates server.

- If the server has no new .DAT file updates or software upgrades, the Online Activity Status dialog box (see Figure A-5 on page 241) tells you that your files are up-to-date. Click **Finish** to disconnect from the server.
- If the server has new .DAT files, the Online Activity Status dialog box (see Figure A-6 on page 242) tells you that the .EXE file containing the .DAT files is automatically downloading to your system.

  When the download is complete, click **Next**. The Online Activity Complete dialog box (see Figure A-7 on page 242) appears.

4. Click **Finish** to install your new .DAT file updates.

If the server has a *product* version more recent than yours, the Newer Component Found dialog box (see Figure A-8 on page 243) appears.

1. To download only the latest .DAT files instead of the entire product, select **DAT files only**, then click **Next**. To download a new product version, click **Next**.
2. The Online Activity Status dialog box (see Figure A-6 on page 242) tracks the status of your download. When your download is complete, click **Next** to continue.

   The Online Activity Complete dialog box (Figure A-11) confirms that your download is complete.

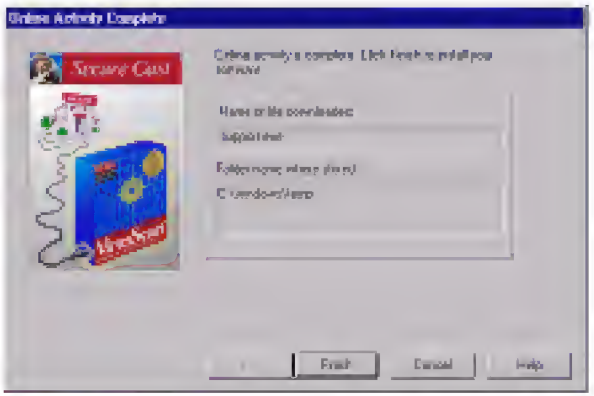

Figure A-11. Online Activity Complete dialog box

3. Note the name and location of the downloaded file, then click **Finish** to install your software.

Registering evaluation software

If you are using a 30-day evaluation version of Network Associates software, the Purchase dialog box (Figure A-12) appears. This dialog box also appears when you choose **Purchase** from the **File** menu in your Network Associates software product.

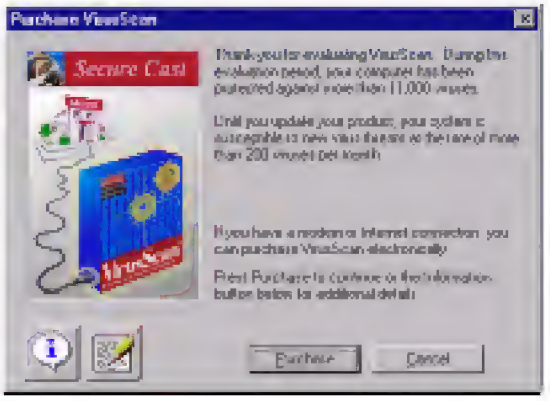

Figure A-12. Purchase dialog box

If you continue to use evaluation copies of Network Associates software after their 30-day licenses expire, you will see increasingly frequent reminders to register your software. Network Associates strongly recommends that you follow these steps to ensure that you are using the newest data files and product versions available:

1. In the Purchase dialog box (Figure A-12), click **Purchase** to begin registering your evaluation copy of anti-virus software electronically.

   The Internet Access dialog box (see Figure A-2 on page 240) appears.

2. If you have Internet access, select **Yes**, then click **Next**. If you do not have Internet access, select **No**, then click **Next**.

   The Server dialog box (see Figure A-4 on page 241) appears. If you selected **Yes**, then the dialup-number box will be unavailable; if you selected **No**, then the dialup-number box will be available.

3. If you have Internet access, verify your Country Code and Area Code, then click **Next**. If you don't have Internet access, verify your Country Code and Area Code, select a modem dialup number, then click **Next**.

   Your system connects to a Network Associates server.

- If the server has no new .DAT file updates or software upgrades, the Online Activity Status dialog box (see Figure A-5 on page 241) tells you that your files are up-to-date. Click **Finish** to disconnect from the server.
- If the server has new .DAT files, the Online Activity Status dialog box (see Figure A-6 on page 242) tells you that the .EXE file containing the .DAT files is automatically downloading to your system.

  When the download is complete, click **Next**. The Online Activity Complete dialog box (see Figure A-7 on page 242) appears.

4. Click **Finish** to install your new .DAT file updates.

If the server has a product version more recent than yours, the Newer Component Found dialog box (see Figure A-8 on page 243) appears. To download only the latest .DAT files instead of the entire product, select **DAT files only**, then click **Next**. To download a new product version, follow these steps:

1. Click **Next** to obtain the newer version of the software.

   If you are no longer entitled to free software upgrades, a second Newer Component Found dialog box (Figure A-13) appears.

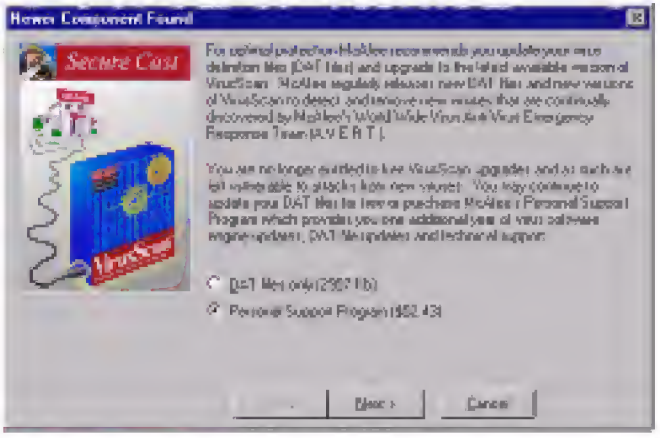

Figure A-13. Newer Component Found dialog box #2

> **NOTE:** File sizes and support pricing are dynamically generated. What you see when you download your purchase, therefore, might vary from what you see in Figure A-13.

2. Click **Next>** to continue with the download.

The Enter Credit Card Information dialog box (Figure A-14) appears.

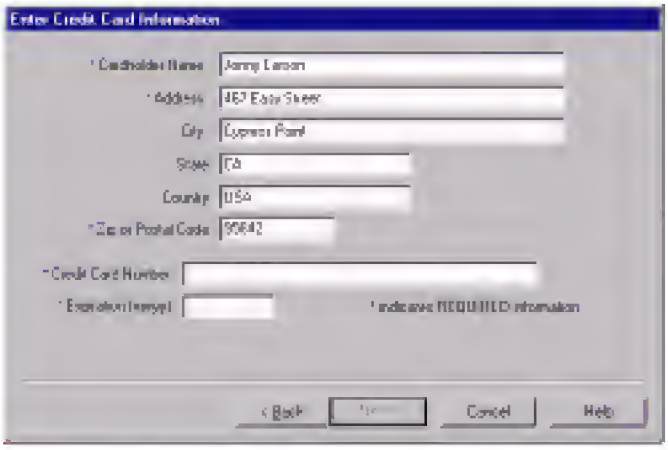

Figure A-14. Enter Credit Card Information dialog box

3. Enter your credit card billing address, account number, and expiration date. Click **Next>** to continue.

> **NOTE:** Your credit card details are safely transmitted in a secure transaction.

The Online Purchase Authorization dialog box (Figure A-15) appears.

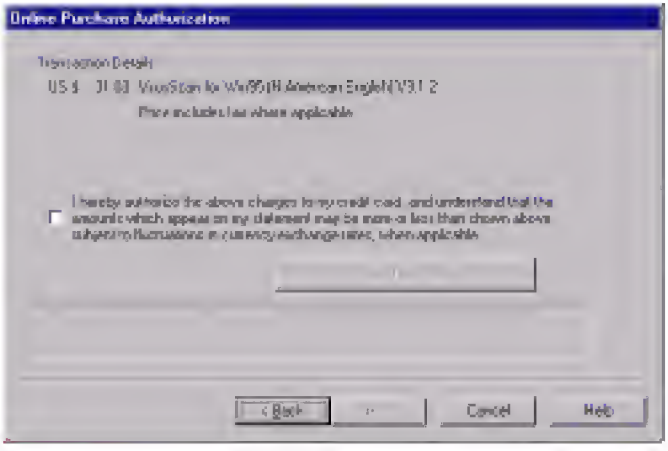

Figure A-15. Online Purchase Authorization dialog box

4. Select the check box to authorize the transaction charges to your credit card, and click Click Here to Buy to begin the download process.

   NOTE: Network Associates will not charge your credit card unless you complete the download successfully.

   The Online Activity Status dialog box (see Figure A-6 on page 242) tracks the status of your download.

5. When your download is complete, note the resulting transaction number for your purchase, then click **Next>** to continue.

   The Online Activity Complete dialog box (see Figure A-9 on page 243) confirms that your transaction is complete.

6. Note the name and location of the downloaded file, then click **Finish** to install your software.

Enterprise SecureCast Channel

If you manage a corporate network, you may download BackWeb's client software from the Network Associates corporate site (http://www.nai.com) and install it on a network server. Enterprise SecureCast is for use by administrators only, not by corporate end users.

NOTE: When the first InfoPak arrives, double-click it to open it, then complete the channel registration process via the Customer Registration Information dialog boxes. When you receive subsequent InfoPak files from Enterprise SecureCast, Network Associates strongly recommends that you distribute them to individual desktops as needed, in order to conserve network bandwidth.

Benefits

- Ease of use

  You no longer have to search for and download updates from Network Associates electronic distribution services. The updates you need will be delivered to you in a zipped format, ready for onsite testing and installation.

- Timely protection

  Network Associates provides you with timely protection by regularly delivering .DAT file updates and product upgrades directly to your desktop. As soon as the updates are released to the SecureCast server, they start to transfer to your site.

- Virus Alerts

  You will receive Virus Alerts that notify you of threatening viruses and suggest the best way to prevent infection. In addition, alerts that distinguish between hoaxes and serious threats will save you valuable time and prevent unnecessary concern.

- Upgrades for multiple platforms

  A subscription to Enterprise SecureCast allows you to receive upgrades and updates to your products for multiple platforms. Data file updates and product upgrades for Network Associates products that run under Windows 95, Windows 98, Windows NT, Windows 3.*x*, DOS, OS/2, and the Mac OS can be delivered to your desktop.

- Localized language versions

  With your subscription, you receive .DAT file updates not only across multiple platforms, but also in the languages of your choice.

- HTTP support in client software

  Enterprise SecureCast supports HTTP (Hypertext Transfer Protocol) for file transmission through your firewall to the SecureCast servers.

> **NOTE:** Firewall considerations: If you have a firewall in place, use HTTP. If you do not, use UDP. If you are using Check Point's Firewall-1™ software, you'll notice that BackWeb is a predefined transmission type.

Setting up Enterprise SecureCast

To obtain the BackWeb client, corporate customers must first have a grant number (product license serial number) to enroll for Enterprise SecureCast.

- If you do not have a grant number, please contact your purchasing agent, your Value Added Reseller, or Network Associates Customer Care at (408) 988-3832 for assistance.
- If you are already a registered Network Associates customer and do not know your grant number, submit the grant-number request form online:

  http://www.nai.com/products/securecast/esc/grantreq.asp

OR

Send an e-mail message to the appropriate address:

ESCRegistration@nai.com (United States)

ESC-Registration-Europe@nai.com (Europe)

ESC-Registration-Asia@nai.com (Asia)

Follow these steps to set up Enterprise SecureCast:

1. Download the Enterprise SecureCast BackWeb client (about 2MB). This client software is specially configured to function in the corporate environment, supporting HTTP file transmission.
2. Install the Enterprise SecureCast client software.

   You will receive a Welcome InfoPak that tells you that your connection to the Enterprise SecureCast channel is working.

3. Begin the channel registration process by entering data about your company in the Customer Registration Information dialog boxes (which will appear in either the first or second InfoPak you receive).

   After you click **Next** on the last registration dialog box, the Online Activity Status dialog box tracks the status of your data transmission.

4. When your user registration is complete, make a note of your registration number, then click **Finish**.

   Your web browser launches showing a product signup form.

5. Select the software, the platforms, and the languages for which you want to receive upgrades and updates.

6. Submit your product signup form.

Using Enterprise SecureCast

You are now ready to receive periodic Virus Alerts, plus product updates and upgrades. Within a few days, you should receive additional InfoPaks. An InfoPak can contain sounds, animations, Web pages, and more. When you receive a new InfoPak from Enterprise SecureCast, it will automatically appear as an animated object on your desktop until you open it. To open an InfoPak, simply double-click it.

Once the updates are on your system, you must distribute them to the workstations on your network. The InfoPaks you receive work well as distribution packages for McAfee Enterprise (Me!) With Me!, you can manage software updates, inventory, distribution, usage metering, and centralized alerting. Contact your Network Associates sales representative for more information about Me!

Troubleshooting Enterprise SecureCast

Registration problems

If you try to register during a busy time of day on the Web, you may encounter a delay when the server tries to process your registration request. If you receive the error message "1105 Error" or "Database Error: Unable to connect to the data source," this means that there is a database problem on the SecureCast server. Try submitting the form again, or try to register later. If you continue to have problems subscribing to the Enterprise SecureCast channel, please contact Network Associates Download Support (Monday to Friday, 8 A.M. to 8 P.M. Central Time) at (972) 278-6100 for assistance.

Firewall problems

Most firewalls that allow web-browsing traffic will also allow you to receive SecureCast InfoPaks. Some firewalls, however, can cause some problems for connections to the SecureCast server. When you complete the registration form and download the software, you will initially download a SecureCast client built with BackWeb version 1.2. Because version 1.2 does not support certain communication protocols, you might see an error similar to "no network connection" when you use it. To correct this problem, download the latest SecureCast client, which was developed with BackWeb version 3.0.

> **NOTE:** You must install the client software that uses BackWeb version 3.0 over the client that uses the 1.2 version of BackWeb. *Do not* uninstall the older version first. This ensures that the new SecureCast client will retain your channel preferences.

Follow these steps to install and configure the newer SecureCast client software:

1. Install BackWeb version 3.0 over BackWeb version 1.2.
2. Start the SecureCast client.
3. To configure the SecureCast client's Communication Method with your own network information, choose **Global Options** from the **Preferences** menu.
4. Change the setting for how BackWeb navigates through your proxy server from **Polite Agent** to **HTTP**. Next, click **HTTP Proxy Setup**, then enter the requested information about your network.

   > **NOTE:** Your proxy server information is specific to your network. If you have further questions, consult your system administrator.

Unsubscribing from Enterprise SecureCast

Follow these steps to cancel this service at any time:

1. Double-click the SecureCast client icon in the Windows taskbar status area.
2. Right-click the **Enterprise** channel button.

   A shortcut menu appears.
3. Click **Unsubscribe**, then click **OK** to confirm.

Support Resources

SecureCast

If you have additional questions about SecureCast, consult the SecureCast FAQ:

http://www.nai.com/products/securecast/esc/enterprise_faq.asp

BackWeb

- For a general description of BackWeb and InfoPaks, read the BackWeb Overview:

  http://www.nai.com/products/securecast/securedetail.asp

- For a comprehensive guide to BackWeb (including additional troubleshooting advice), bookmark the BackWeb User's Manual:

  http://www.backweb.com/doc/version20/Client95/

OR

download the .PDF file:

http://www.backweb.com/doc/version20/bwuser.pdf

- For solutions to serious problems with the operation of BackWeb, please contact Network Associates Download Support (Monday to Friday, 8 A.M. to 8 P.M. Central Time) at (972) 278-6100.

Network Associates Support Services

B

Choosing Network Associates anti-virus and security software helps to ensure that the critical information technology you rely on functions smoothly and effectively. Taking advantage of a Network Associates support plan extends the protection you get from your software by giving you access to the expertise you need to install, monitor, maintain and upgrade your system with the latest Network Associates technology. With a support plan tailored to your needs, you can keep your system or your network working dependably in your computing environment for months or years to come.

Network Associates support plans come under two general headings. If you are a corporate customer, you can choose from three levels of extended support under the Network Associates PrimeSupport program. If you purchased a retail version of a Network Associates product, you can choose a plan geared toward your needs from the Personal Support program.

PrimeSupport Options for Corporate Customers

The Network Associates PrimeSupport program offers a choice of Basic, Extended, or Anytime options. Each option has a range of features that provide you with cost-effective and timely support geared to meet your needs.

PrimeSupport Basic

PrimeSupport Basic gives you telephone access to essential product assistance from experienced Network Associates technical support staff members. If you purchased your Network Associates product with a subscription license, you receive PrimeSupport Basic as part of the package for two years from your date of purchase. If you purchased your Network Associates product with a perpetual license, you can renew your PrimeSupport Basic plan for an annual fee.

PrimeSupport Basic includes these features:

- Telephone access to technical support from Monday through Friday, 8:00 a.m. to 8:00 p.m. Central Time.
- Unrestricted access 24 hours per day to Network Associates technical support information via the Network Associates website.
- Updates to data files and product upgrades via the Network Associates website.

PrimeSupport Extended

PrimeSupport Extended gives you personalized, proactive support from an assigned technical support engineer. You'll enjoy a relationship with a support professional who is familiar with your Network Associates product deployment and support history, and who will call you at an interval you designate to verify that you have the knowledge you need to use and maintain Network Associates products. By calling in advance, your PrimeSupport Extended representative can help to prevent problems before they occur. If, however, an emergency arises, PrimeSupport Extended gives you a committed response time that assures you that help is on the way. You may purchase PrimeSupport Extended on an annual basis when you purchase a Network Associates product either with a subscription license or a perpetual license.

PrimeSupport Extended includes these features:

- Access to an assigned technical support engineer
- Proactive support contacts via telephone or e-mail from your assigned support engineer, at an interval you designate
- Committed response times: your support engineer will respond within one hour to pages, within four hours to voice mail, and within 12 hours to e-mail
- Telephone access to technical support from Monday through Friday, 7:00 a.m. to 7:00 p.m. Central Time
- Unrestricted access 24 hours per day to Network Associates technical support information via the Network Associates website
- Updates to data files and product upgrades via the Network Associates website
- Ability to designate up to five people in your organization as customer contacts

PrimeSupport Anytime

PrimeSupport Anytime offers round-the-clock, personalized, proactive support for Network Associates products deployed in the most business-critical information systems. PrimeSupport Anytime delivers the features of PrimeSupport Extended 24 hours a day, seven days a week, with shorter response time commitments. You may purchase PrimeSupport Anytime on an annual basis when you purchase a Network Associates product, either with a subscription license or a perpetual license.

PrimeSupport Anytime includes these features:

- Access to an assigned technical support engineer
- Proactive support contacts via telephone or e-mail from your assigned support engineer, at an interval you designate
- Committed response times: your support engineer will respond within half an hour to pages, within one hour to voice mail, and within four hours to e-mail
- Telephone access to technical support 24 hours a day, seven days a week
- Unrestricted access 24 hours per day to Network Associates technical support information via the Network Associates website
- Updates to data files and product upgrades via the Network Associates website
- Ability to designate up to 10 people in your organization as customer contacts

Table B-1. PrimeSupport At a Glance

Feature	Basic	Extended	Anytime
Technical support via telephone	Monday–Friday 8:00 a.m.–8:00 p.m.	Monday–Friday 7:00 a.m.–7:00 p.m.	24 hours a day, 7 days a week
Technical support via website	Yes	Yes	Yes
Software updates	Yes	Yes	Yes
Assigned support engineer	—	Yes	Yes
Proactive support contact	—	Yes	Yes
Designated customer contacts	—	5	10
Committed response time	—	Pager: 1 hour Voicemail: 4 hours E-mail: 12 hours	Pager: 30 mins. Voicemail: 1 hour E-mail: 4 hours

Ordering PrimeSupport

To order PrimeSupport Basic, PrimeSupport Extended or PrimeSupport Anytime for your Network Associates products:

- Contact your sales representative; or
- Call Network Associates Support Services at 1-800-988-5737 or 1-650-473-2000 from 6:00 a.m. to 5:00 p.m. Pacific Time, Monday through Friday.

NOTE: The PrimeSupport program described in this guide is available in North America only. To learn about PrimeSupport options available outside North America, contact your regional sales office. Contact information appears near the front of this guide.

Support Services for Retail Customers

If you purchased your Network Associates product through a retail vendor or from the Network Associates website, you also receive some support services as part of your purchase. The specific level of included support depends on the product that you purchased. Examples of the services you receive include:

- Free data (.DAT) file updates for the life of your product via the Network Associates website, your product's AutoUpdate feature, or the SecureCast service (see Appendix A, "Using SecureCast to Update Your Software" for details). You can also update your data files by using your web browser to visit

  http://www.nai.com/download/updates/updates.asp

- Free program (executable file) upgrades for one year via the Network Associates website, your product's AutoUpdate feature, or the SecureCast service (see Appendix A, "Using SecureCast to Update Your Software" for details). If you purchased a deluxe version of a Network Associates product, you receive free program upgrades for two years. You can also upgrade your software by using your web browser to visit:

  http://www.nai.com/download/upgrades/upgrades.asp

- Free access 24 hours a day, seven days a week to online or electronic support through the Network Associates voice and fax system, the Network Associates website, and though such other electronic services as America Online and CompuServe.

To contact Network Associates electronic services, choose one of these options:

- Automated voice and fax system: (408) 988-3034
- Network Associates website: http://support.nai.com
- CompuServe: GO NAI
- America Online: keyword MCAFEE

- Ninety days of complimentary technical support from a Network Associates support technician during regular business hours, Monday through Friday from 8:00 a.m. to 8:00 p.m. Central Time.

After your complimentary support period expires, you can take advantage of a variety of personal support options geared toward your needs. Contact Network Associates Customer Care at (972) 278-6100 to learn more about the options available, or visit the Network Associates website at:

http://www.nai.com/services/support/support.asp.

Network Associates Consulting and Training

Network Associates provides expert consulting and comprehensive education that can help you maximize the security and performance of your network investments through the Network Associates Total Service Solutions program.

Professional Consulting Services

Network Associates Professional Consulting Services is ready to assist during all stages of your network growth, from planning and design, through implementation, and with ongoing management. Network Associates consultants provide an expert supplemental resource and independent perspective to resolve your problems. You'll get help integrating Network Associates products into your environment, along with troubleshooting assistance or help in establishing baselines for network performance. Network Associates consultants also develop and deliver custom solutions to help accomplish your project goals—from lengthy, large-scale implementations to brief problem-solving assignments.

Total Education Services

Network Associates Total Education Services builds and enhances the skills of all network professionals through practical, hands-on instruction that you can take right back to your job. The Total Education Services technology curriculum focuses on network fault and performance management and covers problem solving at all levels. Network Associates also offer modular product training so that you understand the features and functionality of your new software.

You can enroll in Total Education Services courses year-round at Network Associates educational centers, or you can learn from customized courses conducted at your location. All courses follow educational steps along a learning path that takes you to the highest levels of expertise. Network Associates is a founding member of the Certified Network Expert (CNX) consortium.

To learn more about these programs, contact your sales representative or call Total Service Solutions at 1-800-395-3151.

Understanding the .VSC File Format

C

Saving VirusScan task settings

When you choose configuration options for VirusScan, the program saves its settings in the file DEFAULT.VSC, which you'll find in the VirusScan program directory. DEFAULT.VSC is a configuration text file that outlines VirusScan's settings. The file is formatted in a manner similar to Windows .INI files. You can edit this file directly to change the options recorded there—simply open the file with a text editor, such as Windows Notepad. If you have password-protected your VirusScan settings, the program encrypts DEFAULT.VSC to prevent tampering—you must remove the password protection in order to edit the file.

Each variable in the file has a name followed by an equals (=) sign and a value. The values correspond to the settings you selected when you configured VirusScan. The variables are arranged into eight groups that appear under their own headings in DEFAULT.VSC. The tables on the following pages list each variable, along with its default and possible values.

NOTE: Boolean variables can have only 0 and 1 as possible values. A value of 0 tells VirusScan to disable the setting, while 1 enables the setting.

You can distribute copies of your edited DEFAULT.VSC file to other VirusScan users at other computers, overwrite their existing DEFAULT.VSC file, and thereby copy VirusScan's settings for another user to run. VirusScan also allows you to save .VSC files with any name you choose. If you then distribute these files for others to use, the other users would need to locate and double-click them to start VirusScan with the options you encoded into them.

Network Associates also supplies ISeamless, a full-featured configuration and distribution tool that enables you to have complete control over your VirusScan configuration files, including DEFAULT.VSH, DEFAULT.VSC, UPGRADE.INI, UPDATE.INI, and any other special-purpose configuration files you create and save. To learn more about ISeamless and other Network Associates manageability tools, consult your sales representative, or call Network Associates Customer Care.

ScanOptions

Variable	Description
bAutoStart	Type: Boolean (0/1) Instructs VirusScan to automatically start scan when launched Default Value: 0
bAutoExit	Type: Boolean (0/1) Instructs VirusScan to exit automatically when finished scanning if no viruses were found Default Value: 0
bAlwaysExit	Type: Boolean (0/1) Instructs VirusScan to exit automatically when finished scanning even if viruses were found Default Value: 0
bSkipMemoryScan	Type: Boolean (0/1) Instructs VirusScan to skip memory scan Default Value: 0
bSkipBootScan	Type: Boolean (0/1) Instructs VirusScan to skip boot sector scanning Default Value: 0
bSkipSplash	Type: Boolean (0/1) Instructs VirusScan to skip display of the VirusScan splash screen on startup Default Value: 0

DetectionOptions

Variable	Description
bScanAllFiles	Type: Boolean (0/1) Instructs VirusScan to scan all file types Default Value: 0
bScanCompressed	Type: Boolean (0/1) Instructs VirusScan to Scan in compressed files Default Value: 1

Variable	Description
szProgramExtensions	Type: String Specifies which file extensions VirusScan will scan Default Value: EXE COM DO? XL?
szDefaultProgramExtensions	Type: String Specifies default value for szProgramExtensions Default Value: EXE COM DO? XL?

AlertOptions

Variable	Description
bNetworkAlert	Type: Boolean (0/1) Instructs VirusScan to send an alert (.ALR) file to a network path being monitored by NetShield for Centralized Alerting when a virus is found Default Value: 0
bSoundAlert	Type: Boolean (0/1) Instructs VirusScan to sound an audible alert when a virus is detected Default Value: 1
szNetworkAlertPath	Type: String Specifies the network alert path being monitored by NetShield for Centralized Alerting. The folder this path points to should contain the Centralized Alerting file, CENTALRT.TXT Default Value: None

ActionOptions

Variable	Description
bDisplayMessage	Type: Boolean (0/1) Instructs VirusScan to display a message upon detection of a virus Default Value: 0
ScanAction	Type: Integer (0-5) Instructs VirusScan to take the action specified when a virus is detected Possible values: 0 - Prompt for action 1 - Move automatically 2 - Clean automatically 3 - Delete automatically 4 - Continue Default Value: 0
bButtonClean	Type: Boolean (0/1) Instructs VirusScan to display the Clean button if ScanAction=0 Default Value: 1
bButtonDelete	Type: Boolean (0/1) Instructs VirusScan to display the Delete button if ScanAction=0 Default Value: 1
bButtonExclude	Type: Boolean (0/1) Instructs VirusScan to display the Exclude button if ScanAction=0 Default Value: 1
bButtonMove	Type: Boolean (0/1) Instructs VirusScan to display the Move button if ScanAction=0 Default Value: 1
bButtonContinue	Type: Boolean (0/1) Instructs VirusScan to display the Continue button if ScanAction=0 Default Value: 1

Variable	Description
bButtonStop	Type: Boolean (0/1) Instructs VirusScan to display the Stop button if ScanAction=0 Default Value: 1
szMoveToFolder	Type: String Indicates where infected files should be moved Default Value: \Infected
szCustomMessage	Type: String Indicates text of message to be displayed on virus detection Default Value: Possible Virus Detected

ReportOptions

Variable	Description
bLogToFile	Type: Boolean (0/1) Instructs VirusScan to log scan activity to a file Default Value: 1
bLimitSize	Type: Boolean (0/1) Instructs VirusScan to limit the size of the log file Default Value: 1
uMaxKilobytes	Type: Integer (10-999) Specifies maximum size of log file in kilobytes Default Value: 10
bLogDetection	Type: Boolean (0/1) Instructs VirusScan to log virus detection Default Value: 1
bLogClean	Type: Boolean (0/1) Instructs VirusScan to log virus cleaning Default Value: 1
bLogDelete	Type: Boolean (0/1) Instructs VirusScan to log file deletions Default Value: 1

Variable	Description
bLogMove	Type: Boolean (0/1) Instructs VirusScan to log file moves Default Value: 1
bLogSettings	Type: Boolean (0/1) Instructs VirusScan to log session settings Default Value: 1
bLogSummary	Type: Boolean (0/1) Instructs VirusScan to log session summaries Default Value: 1
bLogDateTime	Type: Boolean (0/1) Instructs VirusScan to log date and time of scan activity Default Value: 1
bLogUserName	Type: Boolean (0/1) Instructs VirusScan to log user name Default Value: 1
szLogFileName	Type: String Specifies path to log file Default Value: C:\Program Files\Network Associates\McAfee Viruscan\VSCLOG.TXT

ScanItems

Variable	Description
ScanItem_x, where x is a zero-based index	Type: String Instructs VirusScan to scan the item Default value: `C:|1 *` * The string is separated into fields using the pipe (|) character: Field 1 - Path of item to scan. Field 2 - Boolean (1/0) Possible values: 1 - Instructs VirusScan to scan subfolders of the item 2 - Instructs VirusScan not to scan subfolders of the item

SecurityOptions

Variable	Description
szPasswordProtect	Type: String This variable is not user-configurable Default Value: 0
szPasswordCRC	Type: String This variable is not user-configurable Default Value: 0
szSerialNumber	Type: String This variable is not user-configurable Default Value: 0

ExcludedItems

Variable	Description
NumExcludeItems	Type: Integer (0-n) Defines the number of items excluded from scanning Default value: 1
ExcludedItem_x, where x is a zero-based index	Type: String Instructs VirusScan to exclude the item from scanning Default value: `\Recycled|*.*|1|1 *` * The string is separated into fields using the pipe (|) character: Field 1 - Folder portion of item to exclude. Leave blank for a single file anywhere on the system. Field 2 - File portion of the item to exclude. Leave blank if a folder is excluded without a file name. Field 3 - Integer (1-3) Possible values: 1 - Exclude from file scanning 2 - Exclude from boot-record scanning 3 - Exclude from both boot-record and file scanning Field 4 - Boolean (1/0) Possible values: 1 - Instructs VirusScan to exclude subfolders of the excluded item 2 - Instructs VirusScan to not exclude subfolders

Understanding the .VSH File Format

D

Saving VShield configuration options

When you choose configuration options for VShield, VirusScan saves those settings in the file DEFAULT.VSH, which you'll find in the VirusScan program directory. DEFAULT.VSH is a configuration text file that outlines VShield's settings. The file is formatted in a manner similar to Windows .INI files. You can edit this file directly to change the options recorded there—simply open the file with a text editor, such as Windows Notepad. If you have password-protected your VShield settings, VirusScan encrypts DEFAULT.VSH to prevent tampering—you must remove the password protection in order to edit the file.

Each variable in the file has a name followed by an equals (=) sign and a value. The values correspond to the settings you selected when you configured VShield. The variables are arranged into 24 groups that appear under their own headings in DEFAULT.VSH. Most of these headings correspond to a VShield module. The tables on the following pages list each variable, along with its default and possible values.

NOTE: Boolean variables can have only 0 and 1 as possible values. A value of 0 tells VShield to disable the setting, while 1 enables the setting.

You can distribute copies of your edited DEFAULT.VSH file to other VShield users at other computers, overwrite their existing DEFAULT.VSH file, and thereby copy VShield's settings for another user to run. Network Associates also supplies ISeamless, a full-featured configuration and distribution tool that enables you to have complete control over your VirusScan configuration files, including DEFAULT.VSH, DEFAULT.VSC, UPGRADE.INI, UPDATE.INI, and any other special-purpose configuration files you create and save.

To learn more about ISeamless and other Network Associates manageability tools, consult your sales representative, or call Network Associates Customer Care.

System Scan module

General

Variable	Description
bEnabled	Type: Boolean (1/0) Enables System Scan Default value: 1
bCanBeDisabled	Type: Boolean (1/0) Defines if VShield can be disabled Default value: 1
bShowTaskbarIcon	Type: Boolean (1/0) Defines whether VShield taskbar icon is displayed Default value: 1

DetectionOptions

Variable	Description
bProgFileHeurisitcs	Type: Boolean (1/0) Instructs VShield to scan program files heuristically Default value: 0
bMacroHeuristics	Type: Boolean (1/0) Instructs VShield to scan macros heuristically Default value: 0
bDetectTrojans	Type: Boolean (1/0) Instructs VShield to scan for Trojan viruses Default value: 1
bDetectJoke	Type: Boolean (1/0) Instructs VShield to scan for Joke viruses Default value: 1
bDetectCorrupted	Type: Boolean (1/0) Instructs VShield to scan for corrupted files Default value: 0
bDetectMaybe	Type: Boolean (1/0) Instructs VShield to scan for variants of known viruses Default value: 1

Variable	Description
bRemoveAllMacros	Type: Boolean (1/0) Instructs VShield to delete all macros from infected files Default value: 0
bScanOnExecute	Type: Boolean (1/0) Instructs VShield to scan when files are run Default value: 1
bScanOnOpen	Type: Boolean (1/0) Instructs VShield to scan when files are opened Default value: 1
bScanOnCreate	Type: Boolean (1/0) Instructs VShield to scan when files are created Default value: 1
bScanOnRename	Type: Boolean (1/0) Instructs VShield to scan when files are renamed Default value: 1
bScanOnShutdown	Type: Boolean (1/0) Instructs VShield to scan the boot record of drive A when system is shut down Default value: 1
bScanOnBootAccess	Type: Boolean (1/0) Instructs VShield to scan the boot record of a diskette that was freshly inserted into in the floppy disk drive just before accessing the drive. Default value: 1
bScanAllFiles	Type: Boolean (1/0) Instructs VShield to scan all files, regardless of their extension. Default value: 0
bScanCompressed	Type: Boolean (1/0) Instructs program to scan compressed files Default value: 1

Variable	Description
szProgramExtensions	Type: String Defines the extensions of the files to be scanned Default value: EXE COM DO? XL? MD?, SYS BIN RTF OBD (The ? is a wildcard)
szDefaultProgram Extensions	Type: String Defines extensions to be used as default program extensions during scan configuration Default value: EXE COM DO? XL? MD?, SYS BIN RTF OBD (The ? is a wildcard)

AlertOptions

Variable	Description
bDMIAlert	Type: Boolean (1/0) Enables Desktop Management Interface Alerting Default value: 0
bSoundAlert	Type: Boolean (1/0) Enables audible beep when virus is detected Default value: 1
bNetworkAlert	Type: Boolean (1/0) Enables Centralized Alerting Default value: 0
szNetworkAlertPath	Type: String Specifies a server's Centralized Alerting folder Default value: none

ActionOptions

Variable	Description
bDisplayMessage	Type: Boolean (1/0) Defines if custom message should be displayed in the Prompt for Action dialog box upon virus detection Default value: 0
uVshieldAction	Type: Integer (1-5) Instructs VShield to take the action specified when a virus is detected Possible values: 1 - Prompt user for action 2 - Move infected files automatically 3 - Clean infected files automatically (Deny access if files cannot be cleaned) 4 - Delete infected files automatically 5 - Deny access to infected files and continue Default value: 1
bButtonClean	Type: Boolean (1/0) Instructs VShield to give user option of cleaning file if Prompt for Action is selected and a virus is detected Default value: 1
bButtonDelete	Type: Boolean (1/0) Instructs VShield to give user option of deleting file if Prompt for Action is selected and a virus is detected Default value: 1
bButtonExclude	Type: Boolean (1/0) Instructs VShield to give user option of excluding file if Prompt for Action is selected and a virus is detected Default value: 1
bButtonContinue	Type: Boolean (1/0) Instructs VShield to give user option of continuing the intercepted event if Prompt for Action is selected and a virus is detected Default value: 0
bButtonStop	Type: Boolean (1/0) Instructs VShield to give user option of denying access to the infected file if Prompt for Action is selected and a virus is detected Default value: 1

Variable	Description
szMoveToFolder	Type: String Defines folder to which infected files should be moved Default value: \Infected
szCustomMessage	Type: String Defines custom message to be displayed upon virus detection if action is set to Prompt for Action Default value: None

ReportOptions

Variable	Description
bLogToFile	Type: Boolean (1/0) Defines if results should be logged into log file Default value: 1
bLimitSize	Type: Boolean (1/0) Defines if size of the log file should be limited Default value: 1
uMaxKilobytes	Type: Integer (10-999) Defines maximum size of the log file in kilobytes Default value: 100
bLogDetection	Type: Boolean (1/0) Instructs VShield to log the names of viruses it detects Default value: 1
bLogClean	Type: Boolean (1/0) Defines if cleaning results should be logged Default value: 1
bLogDelete	Type: Boolean (1/0) Defines if infected file delete operations should be logged Default value: 1
bLogMove	Type: Boolean (1/0) Defines if infected file move operations should be logged Default value: 1

Variable	Description
bLogSettings	Type: Boolean (1/0) Instructs VShield to write a record of the settings in use during the scanning session that immediately preceded shutting down your system, or unloading VShield Default value: 1
bLogSummary	Type: Boolean (1/0) Instructs VShield to write a summary of its findings and actions during the scanning session that immediately preceded shutting down your system, or unloading VShield Default value: 1
bLogDateTime	Type: Boolean (1/0) Defines if time and date of an event should be logged Default value: 1
bLogUserName	Type: Boolean (1/0) Defines if user name should be logged Default value: 1
szLogFileName	Type: String Defines log file name Default value: C:\Program Files\Network Associates\McAfee VirusScan\VSHLog.TXT

ExclusionOptions

Variable	Description
szExclusionsFileName	Type: String Default value: C:\Program Files\Network Associates\McAfee VirusScan\VSHLog.TXT

ExcludedItems

Variable	Description
NumExcludedItems	Type: Integer (0-n) Defines the number of items excluded from on-access scanning Default value: 1
ExcludedItem_x, where x is a zero-based index	Type: String Instructs VShield to exclude the item from on-access scanning Default value: \Recycled|*.*|1|1 * * The string is separated into fields using the pipe (|) character: Field 1 - Folder portion of item to exclude. Leave blank for a single file anywhere on the system. Field 2 - File portion of the item to exclude. Leave blank if a folder is excluded without a filename. Field 3 - Integer (1-3) Possible values: 1 - Exclude from file-access scanning 2 - Exclude from boot-record scanning 3 - Exclude from both boot-record and file-access scanning Field 4 - Boolean (1/0) Possible values: 1 - Instructs VShield to exclude subfolders of the excluded item 0 - Instructs VShield to not exclude subfolders

E-Mail Scan module

EMailGeneralOptions

Variable	Description
bMailType	Type: Boolean (1/0) Defines e-mail server type, MAPI or cc:Mail. Default value: 1 (MAPI)
bCanBeDisabled	Type: Boolean (1/0) Prevents disabling of e-mail scanning Default value: 1
bEnabled	Type: Boolean (1/0) Enables e-mail scanning Default value: 0
bEnabledDummy=0	Type: Boolean (1/0) Automatically selects Internet Mail on the E-mail Scan property page when Download Scan is enabled Default value: 0

EMailDetectionOptions

Variable	Description
bScanAllMails	Type: Boolean (1/0) Instructs VShield to scan all new mail Default value: 0
bScanInternetMail	Type: Boolean (1/0) Instructs VShield to scan Internet Mail Default value: 0
bScanAllFiles	Type: Boolean (1/0) Instructs VShield to scan all files Default value: 0
bScanCompressed	Type: Boolean (1/0) Instructs VShield to include compressed files in scan Default value: 1
szProgramExtensions	Type: String Defines the extensions of the files to be scanned Default value: EXE, COM, DO?, XL?, RTF, BIN, SYS, OBD, VXD, MD?, DLL (The ? is a wildcard)

Variable	Description
szDefaultProgram Extensions	Type: String Defines extensions to be used as default program extensions during scan configuration Default value: EXE, COM, DO?, XL?, RTF, BIN, SYS, OBD, VXD, MD?, DLL (The ? is a wildcard)
uPollInterval	Type: Integer (60-999) Defines interval, in seconds, for checking for new mail received via cc:Mail Default value: 60
bDetectTrojans	Type: Boolean (1/0) Instructs VShield to scan for Trojan viruses Default value: 1
bDetectJoke	Type: Boolean (1/0) Instructs VShield to scan for Joke viruses Default value: 1
bDetectCorrupted	Type: Boolean (1/0) Instructs VShield to scan for corrupted files Default value: 0
bDetectMaybe	Type: Boolean (1/0) Instructs VShield to scan for variants of known viruses Default value: 1
bProgFileHeuristics	Type: Boolean (1/0) Instructs VShield to scan program files heuristically Default value: 0
bMacroHeuristics	Type: Boolean (1/0) Instructs VShield to scan macros heuristically Default value: 0

EMailActionOptions

Variable	Description
szMoveFolder	Type: String Defines folder to which infected MAPI e-mail attachments should be moved Default value: \Infected
CC_szMoveFolder	Type: String Defines folder to which infected cc:Mail e-mail attachments should be moved Default value: \Infected
bDisplayMessage	Type: Boolean (1/0) Defines if custom message should be displayed in the Prompt for Action dialog box upon virus detection Default value: 0
uScanAction	Type: Integer (0/3) Instructs VShield to take the action specified when a virus is detected Possible values: 0 - Prompt user for action 1 - Move infected files automatically 2 - Delete infected files automatically 3 - Continue Scanning
bButtonDelete	Type: Boolean (1/0) Instructs VShield to give user option of deleting file if Prompt for Action is selected and a virus is detected Default value: 1
bButtonExclude	Type: Boolean (1/0) Instructs VShield to give user option of excluding file if Prompt for Action is selected and a virus is detected Default value: 0
bButtonMove	Type: Boolean (1/0) Instructs VirusScan to give user option of moving the infected file if Prompt for Action is selected and a virus is detected Default value: 1

Variable	Description
bButtonContinue	Type: Boolean (1/0) Instructs VShield to give user option of continuing the intercepted event if Prompt for Action is selected and a virus is detected Default value: 1
bButtonStop	Type: Boolean (1/0) Instructs VShield to give user option of denying access to the infected file if Prompt for Action is selected and a virus is detected Default value: 0

EMailAlertOptions

Variable	Description
bDMIAlert	Type: Boolean (1/0) Enables Desktop Management Interface Alerting Default value: 0
bNetworkAlert	Type: Boolean (1/0) Enables Centralized Alerting Default value: 0
szNetworkAlertPath	Type: String Specifies a server's Centralized Alerting folder Default value: none
szCustomMessage	Type: String Defines custom message to be displayed upon virus detection if action is set to Prompt for Action Default value: McAfee VShield: Virus found in attachment!
bReturnMail	Type: Boolean (1/0) Instructs VShield to notify sender of infected e-mail that was received via a MAPI client Default value: 0
szReturnCc	Type: String Identifies recipient(s) of copy of notification to sender of infected e-mail that was received via a MAPI client Default value: none

Variable	Description
szReturnSubject	Type: String Allows insertion of Subject text for notification to sender of infected e-mail that was received via a MAPI client Default value: none
szReturnBody	Type: String Allows inclusion of message text in notification to sender of infected e-mail that was received via a MAPI client Default value: none
bSendMailToUser	Type: Boolean (1/0) Instructs VShield to notify other users of infected e-mail that was received via a MAPI client Default value: 0
szSendTo	Type: String Identifies other users who should receive notification of infected e-mail that was received via a MAPI client Default value: none
szSendCc	Type: String Identifies people who should receive copies of the notification to other users about infected e-mail that was received via a MAPI client Default value: none
szSendSubject	Type: String Allows insertion of Subject text for notification to others of infected e-mail that was received via a MAPI client Default value: none
szSendBody	Type: String Allows inclusion of message text in notification to others of infected e-mail that was received via a MAPI client Default value: none
CC_bReturnMail	Type: Boolean (1/0) Instructs VShield to notify sender of infected e-mail that was received via cc:Mail Default value: 0
CC_bSendMailToUser	Type: Boolean (1/0) Instructs VShield to notify other users of infected e-mail that was received via cc:Mail Default value: 0

Variable	Description
CC_szReturnCc	Type: String Identifies recipient(s) of copy of notification to sender of infected e-mail that was received via cc:Mail Default value: none
CC_szReturnSubject	Type: String Allows insertion of Subject text for notification to sender of infected e-mail that was received via cc:Mail Default value: none
CC_szReturnBody	Type: String Allows inclusion of message text in notification to sender of infected e-mail that was received via cc:Mail Default value: none
CC_szSendTo	Type: String Identifies other users who should receive notification of infected e-mail that was received via cc:Mail Default value: none
CC_szSendCc	Type: String Identifies people who should receive copies of the notification to other users about infected e-mail that was received via cc:Mail Default value: none
CC_szSendSubject	Type: String Allows insertion of Subject text for notification to others of infected e-mail that was received via cc:Mail Default value: none
CC_szSendBody	Type: String Allows inclusion of message text in notification to others of infected e-mail that was received via cc:Mail Default value: none

EMailReport Options

Variable	Description
bLogToFile	Type: Boolean (1/0) Defines if scan results should be logged into log file Default value: 1
bLimitSize	Type: Boolean (1/0) Defines if size of the log file should be limited Default value: 1
uMaxKilobytes	Type: Integer (10-999) Defines maximum size of the log file in kilobytes Default value: 100
bLogDetection	Type: Boolean (1/0) Instructs VShield to log the names of viruses it detects Default value: 1
bLogClean	Type: Boolean (1/0) Defines if cleaning results should be logged Default value: 1
bLogDelete	Type: Boolean (1/0) Defines if infected file delete operations should be logged Default value: 1
bLogMove	Type: Boolean (1/0) Defines if infected file move operations should be logged Default value: 1
bLogSettings	Type: Boolean (1/0) Instructs VShield to write a record of the settings in use during the scanning session that immediately preceded shutting down your system, or unloading VShield Default value: 1
bLogSummary	Type: Boolean (1/0) Instructs VShield to write a summary of its findings and actions during the scanning session that immediately preceded shutting down your system, or unloading VShield Default value: 1

Variable	Description
bLogDateTime	Type: Boolean (1/0) Defines if time and date of an event should be logged Default value: 1
bLogUserName	Type: Boolean (1/0) Defines if user name should be logged Default value: 1
szLogFileName	Type: String Defines log file name Default value: C:\Program Files\Network Associates\McAfee VirusScan\WebEmail.txt

Download Scan module

DownloadGeneralOptions

Variable	Description
bEnabled	Type: Boolean (1/0) Enables scanning of downloaded files Default value: 1
bCanBeDisabled	Type: Boolean (1/0) Prevents disabling the scanning of downloaded files Default value: 1

DownloadDetectionOptions

Variable	Description
bScanAllFiles	Type: Boolean (1/0) Instructs VShield to scan all files Default value: 0
bScanCompressed	Type: Boolean (1/0) Instructs VShield to include compressed files in scan Default value: 1
bDetectTrojans	Type: Boolean (1/0) Instructs VShield to scan for Trojan viruses Default value: 1

Variable	Description
bDetectJoke	Type: Boolean (1/0) Instructs VShield to scan for Joke viruses Default value: 1
bDetectCorrupted	Type: Boolean (1/0) Instructs VShield to scan for corrupted files Default value: 0
bDetectMaybe	Type: Boolean (1/0) Instructs VShield to scan for variants of known viruses Default value: 1
bProgFileHeuristics	Type: Boolean (1/0) Instructs VShield to scan program files heuristically Default value: 0
bMacroHeuristics	Type: Boolean (1/0) Instructs VShield to scan macros heuristically Default value: 0
szProgramExtensions	Type: String Defines the extensions of the files to be scanned Default value: EXE, COM, DO?, XL?, RTF, BIN, SYS, OBD, VXD, MD?, DLL (The ? is a wildcard)

DownloadActionOptions

Variable	Description
szMoveToFolder	Type: String Defines folder to which infected files should be moved Default value: \Infected
szCustomMessage	Type: String Defines custom message to be displayed upon virus detection if action is set to Prompt for Action Default value: McAfee VShield: Virus found in download file!

Variable	Description
uScanAction	Type: Integer (0/3) Instructs VShield to take the action specified when a virus is detected Default value: 0 Possible values: 0 - Prompt user for action 1 - Move infected files automatically 2 - Delete infected files automatically 3 - Continue Scanning
bButtonClean	Type: Boolean (1/0) Instructs VShield to give user option of cleaning file if Prompt for Action is selected and a virus is detected Default value: 1
bButtonDelete	Type: Boolean (1/0) Instructs VShield to give user option of deleting file if Prompt for Action is selected and a virus is detected Default value: 1
bButtonExclude	Type: Boolean (1/0) Instructs VShield to give user option of excluding file if Prompt for Action is selected and a virus is detected Default value: 0
bButtonMove	Type: Boolean (1/0) Instructs VirusScan to give user option of moving the infected file if Prompt for Action is selected and a virus is detected Default value: 1
bButtonContinue	Type: Boolean (1/0) Instructs VShield to give user option of continuing the intercepted event if Prompt for Action is selected and a virus is detected Default value: 1
bButtonStop	Type: Boolean (1/0) Instructs VShield to give user option of denying access to the infected file if Prompt for Action is selected and a virus is detected Default value: 0

DownloadAlertOptions

Variable	Description
bDMIAlert	Type: Boolean (1/0) Enables Desktop Management Interface Alerting Default value: 0
bNetworkAlert	Type: Boolean (1/0) Enables Centralized Alerting Default value: 0
szNetworkAlertPath	Type: String Specifies a server's Centralized Alerting folder Default value: none
bSoundAlert	Type: Boolean (1/0) Enables audible beep when virus is detected Default value: 1
bDisplayMessage	Type: Boolean (1/0) Defines if custom message should be displayed in the Prompt for Action dialog box upon detection of a hostile ActiveX control or Java applet, or an attempt to connect to a banned URL or IP address. Default value: 0

DownloadReportOptions

Variable	Description
bLogToFile	Type: Boolean (1/0) Defines if scan results should be logged into log file Default value: 1
bLimitSize	Type: Boolean (1/0) Defines if size of the log file should be limited Default value: 1
uMaxKilobytes	Type: Integer (10-999) Defines maximum size of the log file in kilobytes Default value: 100
bLogDetection	Type: Boolean (1/0) Instructs VShield to log hostile ActiveX control or Java applet it encounters, or attempts to connect to a banned URL or IP address. Default value: 1

Variable	Description
bLogClean	Type: Boolean (1/0) Defines if cleaning results should be logged Default value: 1
bLogDelete	Type: Boolean (1/0) Defines if infected file delete operations should be logged Default value: 1
bLogMove	Type: Boolean (1/0) Defines if infected file move operations should be logged Default value: 1
bLogSettings	Type: Boolean (1/0) Instructs VShield to write a record of the settings in use during the scanning session that immediately preceded shutting down your system, or unloading VShield Default value: 1
bLogSummary	Type: Boolean (1/0) Instructs VShield to write a summary of its findings and actions during the scanning session that immediately preceded shutting down your system, or unloading VShield Default value: 1
bLogDateTime	Type: Boolean (1/0) Defines if time and date of an event should be logged Default value: 1
bLogUserName	Type: Boolean (1/0) Defines if user name should be logged Default value: 1
szLogFileName	Type: String Defines log file name Default value: C:\Program Files\Network Associates\McAfee VirusScan\WebInet.txt

Internet Filter module

INetFltrGeneralOptions

Variable	Description
bEnabled	Type: Boolean (1/0) Enables scanning of downloaded files Default value: 1
bCanBeDisabled	Type: Boolean (1/0) Prevents disabling the scanning of downloaded files Default value: 1

INetFltrDetectionOptions

Variable	Description
bScanIP	Type: Boolean (1/0) Instructs VShield to block designated IP addresses Default value: 1
bScanHost	Type: Boolean (1/0) Instructs VShield to block designated URLs Default value: 1
bScanJava	Type: Boolean (1/0) Instructs VShield to scan for potentially harmful Java applets Default value: 1
bScanActiveX	Type: Boolean (1/0) Instructs VShield to scan for potentially harmful ActiveX objects Default value: 1
bDetectTrojans	Type: Boolean (1/0) Instructs VShield to scan for Trojan viruses Default value: 1
bDetectJoke	Type: Boolean (1/0) Instructs VShield to scan for Joke viruses Default value: 1
bDetectCorrupted	Type: Boolean (1/0) Instructs VShield to scan for corrupted files Default value: 0

Variable	Description
bDetectMaybe	Type: Boolean (1/0) Instructs VShield to scan for variants of known viruses Default value: 1
bProgFileHeuristics	Type: Boolean (1/0) Instructs VShield to scan program files heuristically Default value: 0
bMacroHeuristics	Type: Boolean (1/0) Instructs VShield to scan macros heuristically Default value: 0

INetFltrActionOptions

Variable	Description
uScanAction	Type: Integer (0/1) Instructs VShield to take the action specified when a banned URL, IP address, ActiveX control, or Java applet is detected Default value: 0 Possible values: 0 - Prompt user for action 1 - Deny Access to objects

INetFltrAlertOptions

Variable	Description
bDMIAlert	Type: Boolean (1/0) Enables Desktop Management Interface Alerting Default value: 0
bNetworkAlert	Type: Boolean (1/0) Enables Centralized Alerting Default value: 0
szNetworkAlertPath	Type: String Specifies a server's Centralized Alerting folder Default value: none

Variable	Description
bDisplayMessage	Type: Boolean (1/0) Defines if custom message should be displayed in the Prompt for Action dialog box upon virus detection Default value: 0
bSoundAlert	Type: Boolean (1/0) Enables audible beep when a banned URL, IP address, ActiveX control, or Java applet is detected Default value: 1
szCustomMessage	Type: String If action is set to Prompt for Action, this variable defines custom message to be displayed when a banned URL, IP address, ActiveX control, or Java applet is detected Default value: McAfee VShield: Hostile internet object or banned site detected!

INetFltrReportOptions

Variable	Description
bButtonDeny	Type: Boolean (1/0) Instructs VShield to give user option of denying access to the site where the potentially dangerous object was detected Default value: 1
bButtonContinue	Type: Boolean (1/0) Instructs VShield to give user option of continuing the intercepted event if Prompt for Action is selected and a banned URL, IP address, ActiveX control, or Java applet is detected Default value: 1
bLogToFile	Type: Boolean (1/0) Defines if scan results should be logged into log file Default value: 1
bLimitSize	Type: Boolean (1/0) Defines if size of the log file should be limited Default value: 1
uMaxKilobytes	Type: Integer (10-999) Defines maximum size of the log file in kilobytes Default value: 100

Variable	Description
bLogDetection	Type: Boolean (1/0) Instructs VShield to log the names of viruses it detects Default value: 1
bLogSettings	Type: Boolean (1/0) Instructs VShield to write a record of the settings in use during the scanning session that immediately preceded shutting down your system, or unloading VShield Default value: 1
bLogSummary	Type: Boolean (1/0) Instructs VShield to write a summary of its findings and actions during the scanning session that immediately preceded shutting down your system, or unloading VShield Default value: 1
bLogDateTime	Type: Boolean (1/0) Defines if time and date of an event should be logged Default value: 1
bLogUserName	Type: Boolean (1/0) Defines if user name should be logged Default value: 1
szLogFileName	Type: String Defines log file name Default value: C:\Program Files\Network Associates\McAfee VirusScan\WebFiltr.txt

Security module

SecurityOptions

Variable	Description
bPasswordEnabled	Type: Boolean (1/0) Defines if password protection is enabled Default value: 0
szPasswordCRC	Reserved. Do not modify
bProtectAllOptions	Type: Boolean (1/0) Defines if all property pages are password protected Default value: 1
szPasswordProtect	Reserved. Do not modify

General Settings

AVCONFILE

Variable	Description
AVCONFILE	Type: String Specifies the path to AVCONSOLE Default: C:\Program Files\Network Associates\McAfee VirusScan\avconsol.ini
SECTION	Type: String Specifies the reporting location within AVCONSOL.INI Default: Item_0

Using VirusScan Command-Line Options

E

Running VirusScan Command line

You can run VirusScan Command Line either from a Windows MS-DOS Prompt window, or by restarting your computer in DOS mode. Network Associates recommends restarting in DOS mode for best results. To learn how to restart your computer in DOS mode, see your Microsoft Windows documentation.

To run VirusScan Command line, follow these steps:

1. Open an MS-DOS Prompt window from within Windows, or restart your computer in DOS mode.
2. Change to the VirusScan program directory. If you installed VirusScan with its default options, type this line at your command prompt to locate the correct directory:

   ```
   C:\progra~1\networ~1\mcafee~1
   ```

3. Type `scan`, followed by the scan options you want to use, at the command prompt.

   VirusScan Command Line will start immediately and begin scanning your system with the options you choose. When it has finished, it will display the results of its scan operation, then return to the command prompt.

4. To run another scan operation, repeat Step 3. To close the MS-DOS Prompt window, type `exit` at the command prompt. If you restarted your computer in DOS mode, type `win` to start Windows, or restart your computer as you would normally.

The tables on the following pages list all of the VirusScan options available.

NOTE: When you specify a file name as part of a command-line option, you must include the full path to the file if it is not located in the VirusScan program directory.

Command line options

Command Line Option	Limitations	Description
All the options listed below can be used to configure both on-demand and on-access scans, unless otherwise noted.		
/? or /HELP	None.	Displays a list of VirusScan command-line options, each with a brief description.
/ADL	On-demand scanning option only.	Scan all local drives—including compressed drives and PC cards, but not disks—in addition to any other drive(s) specified on the command line. To scan both local and network drives, use the /ADL and /ADN commands together in the same command line. OS/2: /ADL includes the CD-ROM drive in the scan, when used with /NODDA.
/ADN	On-demand scanning option only.	Scan all network drives—including CD-ROM—for viruses, in addition to any other drive(s) specified on the command line. *Note:* To scan both local drives and network drives, use the /ADL and /ADN commands together in the same command line.
/ALERTPATH *<dir>*	On-demand scanning option only.	Designates the directory *<dir>* as a network path monitored by Centralized Alerting.
/ALL	On-demand scanning option only.	Overrides the default scan setting by scanning all infectable files—regardless of extension. *Notes:* Using the /ALL option substantially increases the scanning time required. Use it only if you find a virus or suspect that you have one. By default, VirusScan only scans files with the following extensions: .EXE, .COM, .SYS, .BIN, .OVL, .DLL, .DOC, .DOT, .XLA, .XLS, .XLT, .RTF, and .VXD. These are the file types that are most susceptible to viruses.
/ANALYZE	On-demand scanning option only. Extended memory required.	Sets VirusScan to scan using its full heuristics, both program and macro. *Note:* /MANALYZE targets macro viruses only; /PANALYZE targets program viruses only.

Command Line Option	Limitations	Description
/ANYACCESS	On-access scanning option only.	Scans: * the boot sector whenever a disk is either read or written to * executables * any newly created files.
/APPEND	On-demand scanning option only.	Used with /REPORT to append report message text to the specified report file instead of overwriting it.
/BOOT	On-demand scanning option only.	Scan boot sector and master boot record only.
/BOOTACCESS	On-access scanning option only.	Scans a disk's boot sector for viruses whenever the disk is accessed (including read/write operations).
/CLEAN	On-demand scanning option only.	Clean viruses from all infected files and system areas.
/CLEANDOCALL	On-demand scanning option only.	As a precautionary measure against macro viruses, /CLEANDOCALL cleans all macros from Microsoft Word and Office documents. *Note:* This option deletes all macros, including macros not infected by a virus.
/CONTACT *<message>*	On-access scanning option only.	Displays specified message when a virus is detected. This message cannot exceed 255 characters.
/CONTACTFILE *<filename>*	None.	Display the contents of *<filename>* when a virus is found. It is an opportunity to provide contact information and instructions to the user when a virus is encountered. This option is especially useful in network environments, because you can easily maintain the message text in a central file rather than on each workstation. *Note:* Any character is valid in a contact message except a backslash (\). Messages beginning with a slash (/)or a hyphen (-) should be placed in quotation marks.
/DEL	On-demand scanning option only.	Deletes infected files permanently.

Command Line Option	Limitations	Description
/EXCLUDE *<filename>*	On-demand scanning option only.	Do not scan or add validation codes to the files listed in *<filename>*. Use this option to: * Exclude specific files from a scan. List the complete path to each file that you want to exclude on its own line. You may use wildcards * and ?
/FILEACCESS	On-access scanning option only.	Scans executable files on access as well as execution. *Note:* This scan will *not* check the boot sector.
/FREQUENCY *<n>*	On-demand scanning option only.	Do not scan *<n>* hours after the previous scan. In environments where the risk of viral infection is very low, use this option to prevent unnecessary scans. Remember, the greater the scan frequency, the greater your protection against infection.
/HELP or /?	None.	Displays a list of VirusScan command-line options, each with a brief description.
/IGNORE *<drive(s)>*	On-access scanning option only.	Does not check any files loaded from the specified drive(s).
/LOAD *<filename>*	On-demand scanning option only.	Load scanning options from the named file. Use this option to perform a scan you've already configured by loading custom settings saved in an ASCII-formatted file.
/LOCK	Not available in low-memory environments	With this /LOCK option enabled, VirusScan will halt and lock your system if it finds a virus. /LOCK is appropriate in highly vulnerable network environments, such as open-use computer labs. Network Associates recommends using /LOCK with the /CONTACTFILE option to tell users what to do or whom to contact if VirusScan locks the system.
/MANALYZE	On-demand scanning option only. Extended memory required.	Sets VirusScan's heuristic scanning features to target macro viruses only. *Note:* /PANALYZE targets program viruses only; /ANALYZE targets both program and macro viruses.

Command Line Option	Limitations	Description
/MANY	On-demand scanning option only.	Scans multiple disks consecutively in a single drive. VirusScan will prompt you for each disk. Use this option to check multiple floppy disks quickly. You cannot use the /MANY option if you run VirusScan from a boot disk and you have only one floppy drive.
/MAXFILESIZE *<xxx.x>*	On-demand scanning option only.	Scan only files no larger than *<xxx.x>* megabytes.
/MEMEXCL		Excludes the memory address A0000:0000 from scanning.
/MOVE *<dir>* or *.???	On-demand scanning option only.	*/MOVE <directory>:* Moves all infected files found during a scan to the specified directory, preserving drive letter and directory structure. *Note:* This option has no effect if the Master Boot Record or boot sector is infected, since these are not actually files. */MOVE*.???:* VirusScan will change the extension of infected files, but not move them. For example, using the /MOVE*.BAD option will result in any infected files being simply renamed with the extension .BAD but not physically moved.
/NOBEEP	On-demand scanning option only.	Disables the tone that sounds whenever VirusScan finds a virus.
/NOBREAK	On-demand scanning option only.	Disables CTRL-C and CTRL-BREAK during scans. Users will not be able to halt scans in progress with /NOBREAK in use.
/NOCOMP	On-demand scanning option only. Extended memory required.	Skips checking of compressed executables created with the LZEXE or PkLite file-compression programs. This reduces scanning time when a full scan is not needed. Otherwise, by default, VirusScan checks inside executable, or self-decompressing, files by decompressing each file in memory and checking for virus signatures. VirusScan will still check for modifications to compressed executables if they contain VirusScan validation codes.

Command Line Option	Limitations	Description
/NODDA	On-demand scanning option only.	No direct disk access. This prevents VirusScan from accessing the boot record. This feature has been added to allow VirusScan to run under Windows NT. You might need to use this option on some device-driven drives. Using /NODDA with the /ADN or /ADL switches may generate errors when accessing empty CD-ROM drives or empty Zip drives. If this occurs, type F (for Fail) in response to the error messages to continue the scan.
/NODISK	On-access scanning option only.	Does not scan boot sector while loading VShield.
/NODOC	On-demand scanning option only.	Does not scan Microsoft Office files.
/NOEMS	On-access scanning option only.	Keeps VShield from using expanded memory (EMS).
/NOEXPIRE	On-demand scanning option only.	Disables the “expiration date” message if the VirusScan data files are out of date.
/NOMEM	None.	Does not scan memory for viruses. This greatly reduces scan time. Use /NOMEM only when you are absolutely certain that your computer is virus-free.
/NOREMOVE	On-access scanning option only.	Prevents VShield from being removed from memory with the /REMOVE switch.
/NOWARMBOOT	On-access scanning option only.	Does not check the disk boot sector of the floppy disk in the A: drive for viruses during warm boot (system reset or CTRL+ALT+DEL).
/NOXMS	On-access scanning option only.	Does not use extended memory (XMS).
/ONLY *<drive(s)>*	On-access scanning option only.	Checks only files loaded from the specified drive(s).

Command Line Option	Limitations	Description
/PANALYZE	On-demand scanning option only. Extended memory required.	Sets VirusScan to scan using program heuristics. *Note:* /MANALYZE targets macro viruses only; /ANALYZE targets both program and macro viruses.
/PAUSE	On-demand scanning option only.	Enables screen pause. The "Press any key to continue" prompt will appear when VirusScan fills a screen with messages. Otherwise, by default, VirusScan fills and scrolls a screen continuously without stopping, which allows VirusScan to run on PCs with multiple drives or that have severe infections without needing your input. Network Associates recommends omitting /PAUSE when using the report options (/REPORT, /RPTCOR, and /RPTERR).
/PLAD	On-demand scanning option only.	Preserves the last access dates on Novell NetWare drives. Normally, proprietary network drives update the last access date when VirusScan opens and examines a file. However, some tape backup systems use this last access date to decide whether to back up the file. Use /PLAD to ensure that the last access date does not change as the result of scanning.
/RECONNECT	On-access scanning option only.	Restores VShield after it has been disabled by certain drivers or memory-resident programs.
/REMOVE	On-access scanning option only.	Unloads VShield from memory.

Command Line Option	Limitations	Description
/REPORT *<filename>*	On-demand scanning option only.	Creates a report of infected files and system errors, and saves the data to *<filename>* in ASCII text file format. If *<filename>* already exists, /REPORT will overwrite it. To avoid overwriting, use the /APPEND option with /REPORT: VirusScan will instead add report information to the end of the file, instead of overwriting it. You can also use /RPTALL, /RPTCOR, and /RPTERR to add scanned files, corrupted files, modified files, and system errors to the report. You can include the destination drive and directory (such as D:\VSREPRT\ALL.TXT), but if the destination is a network drive, you must have rights to create and delete files on that drive. Network Associates recommends omitting /PAUSE when using any report option.
/RPTALL	On-demand scanning option only.	Include all scanned files in the /REPORT file. When used with /REPORT, this option adds the names of corrupted files to the report file. You can use /RPTCOR with /RPTERR on the same command line. Network Associates recommends omitting /PAUSE when using any report option.
/RPTCOR	On-demand scanning option only.	Include corrupted files in /REPORT file. When used with /REPORT, this option adds the names of corrupted files to the report file. Corrupted files that VirusScan finds may have been damaged by a virus. You can use /RPTCOR with /RPTERR on the same command line. There may be false readings in some files that require an overlay or another executable to run properly (that is, a file that is not executable on its own). Network Associates recommends omitting /PAUSE when using any report option.

Command Line Option	Limitations	Description
/RPTERR	On-demand scanning option only.	Include errors in /REPORT file. When used with /REPORT, this option adds a list of system errors to the report file. /LOCK is appropriate in highly vulnerable network environments, such as open-use computer labs. You can use /RPTERR with /RPTCOR on the same command line. System errors can include problems reading or writing to a disk or hard disk, file system or network problems, problems creating reports, and other system-related problems. Network Associates recommends omitting /PAUSE when using any report option.
/SAVE	On-access scanning option only.	Saves the command-line options to the VSHIELD.INI file.
/SUB	On-demand scanning option only.	Scans subdirectories inside a directory. By default, when you specify a directory to scan rather than a drive, VirusScan will examine only the files it contains, not its subdirectories. Use /SUB to scan all subdirectories within any directories you have specified. It is not necessary to use /SUB if you are scanning an entire drive.
/UNZIP	On-demand scanning option only. Extended memory required.	Scan inside compressed files.

Command Line Option	Limitations	Description
/VIRLIST	On-demand scanning option only.	Displays the name and a brief description of each virus that VirusScan detects. You may use the /PAUSE option on the same command line as /VIRLIST to read the virus list one screen at a time. *To redirect the /VIRLIST output to a text file:* At the command prompt, type: scan /VIRLIST> filename.txt Because VirusScan can detect many viruses, this file will be over 250 pages long. This is too large for the MS-DOS "Edit" program to open; Network Associates recommends using Notepad or another text editor to open the virus list.
/XMSDATA	On-access scanning option only.	Loads VShield data files into XMS memory.

Index

A

action options, choosing
- for VirusScan in Scheduler, 183 to 186
- in Download Scan module, 112 to 114
- in E-mail Scan module, 102 to 104
- in Internet Filter module, 123 to 124
- in System Scan module, 87 to 90
- in the E-Mail Scan program component, 222 to 224
- in VirusScan Advanced, 154 to 156
- in VirusScan Classic, 146 to 147

ActiveX controls
- as malicious software, xviii to xix, 27
- detecting with VShield's Internet Filter module, 118 to 120
- distinction between viruses and, xix

alarms, false, understanding, 71 to 72

alert messages
- audible, sounding, 92, 107, 116, 125, 149, 158, 188, 227
- Centralized Alerting, 91, 105, 115, 125, 157, 187, 225
- custom, displaying, 92, 107, 116, 125, 158, 188, 227
- sending to your network administrator, 91, 105, 115, 125, 157, 187, 225
- sending via DMI, 91, 107, 115, 125, 157, 187, 227
- settings in .VSC file for Centralized Alerting, 263

alert options, choosing
- for VirusScan in Scheduler, 186 to 188
- in Download Scan module, 114 to 116
- in E-mail Scan module, 104 to 108
- in Internet Filter module, 124 to 125
- in System Scan module, 90 to 92
- in the E-Mail Scan program component, 225 to 227
- in VirusScan Advanced, 156 to 160

America Online
- mail client, supported in VShield, 74
- technical support via, xxi, 259

anonymous FTP, use of to log on to update and upgrade sites, 202, 212

anti-virus software
- code signatures, use of for virus detection, xvii
- consequences of running multiple vendor versions, 71 to 72
- reporting new viruses not detected by to Network Associates, xxiii

audible alert messages, sounding, 92, 107, 116, 125, 149, 158, 188, 227

authenticating Network Associates files, use of VALIDATE.EXE for, 50 to 51

automatic start, setting for scan task, 183

AutoUpdate
- advanced options for, configuring, 203 to 205
- Force Update, use of to replace corrupted .DAT files, 204
- number of connection attempts made for update sites, 202
- options for, configuring, 196 to 205
- settings file for, 201, 203, 205

use of in conjunction with Enterprise SecureCast, 196

AutoUpgrade

advanced options for, configuring, 213 to 214

number of connection attempts made for upgrade sites, 212

options for, configuring, 206 to 214

settings file for, 211, 213 to 214

use of in conjunction with Enterprise SecureCast, 206

B

background scan tasks, configuring

in configuration wizard, 77

in ScreenScan, 230 to 234

in System Scan Properties dialog box, 81 to 97

Basic, as macro virus programming language, xviii

batch files, running after successful updates, 205

BIOS

possible VirusScan conflicts with anti-virus features of, 72

boot blocks

scanning, 183

boot record

preventing VirusScan from accessing, 300

boot sector

limiting scan operations to, 297

omitting from scanning during a warm boot, 300

BOOTSCAN.EXE

use of on Emergency Disk, 54

boot-sector viruses, definition and behavior of, xv to xvi

"Brain" virus, xv

browsers supported in VShield, 74

C

.CAB (Compressed Application Binary) files, scanning, 101, 112, 144, 152, 180, 220, 232

cc:Mail

as e-mail client supported in VShield, 74

choosing correct options for

in configuration wizard, 78

in E-mail Scan Properties dialog box, 99

logging on to and scanning v6.0 and v7.0 mailboxes, 229 to 230

CENTALRT.TXT, 91, 105, 115, 125, 157, 187, 225

Centralized Alerting, settings for in .VSC file, 263

checking files with VALIDATE.EXE, 50 to 51

clean

all infected files, 297

all macros from Microsoft Word and Office files, 297

code signatures

use of by viruses, xvii

COMMAND.COM files, virus infections in, xvi

components, included with VirusScan, 28 to 30

compressed files

scanning, 83, 101, 112, 144, 152, 180, 220, 232

skipping during scan operations, 299

CompuServe, technical support via, xxi, 259

computer problems, attributing to viruses, 53
Concept virus, introduction of, xvii to xviii
configuration
choosing options for VirusScan in Scheduler, 176 to 195
of E-Mail program component, 218 to 229
of ScreenScan, 230 to 234
of VirusScan Advanced, 149 to 164
of VirusScan Classic, 143 to 149
of VShield
in Download Scan module, 110 to 118
in E-mail Scan module, 97 to 109
in Internet Filter module, 118 to 128
in Security module, 128 to 132
in System Scan module, 82 to 97
using wizard, 75 to 81
configuration wizard
Download Scan module options, choosing with, 79
E-mail Scan module options, choosing with, 78
Internet Filter module options, choosing with, 80
starting, 75
System Scan module options, choosing with, 77
using, 75 to 81
consulting services, 259
contents of log file, 94, 109, 117, 160, 190, 228
context menus
use of in VirusScan Scheduler window, 166
Copy
in **Edit** menu, 167
corporate e-mail systems, choosing
in configuration wizard, 78
in E-Mail Scan Properties dialog box, 99 to 100
costs from virus damage, xiii to xiv
crashes, when not attributable to viruses, 31 to 32
CTRL+ALT+DEL, ineffective use of to clear viruses, xvi
CTRL+BREAK
disabling during scan operations, 299
CTRL+C
disabling during scan operations, 299
custom alert message, displaying, 92, 107, 116, 125, 158, 188, 227
Customer Care
contacting, xxi

D

damage from viruses, xiii
payloads, xv
.DAT file updates
reporting new items for, xxiii
definition of and numbering convention for, 196
data files
additional, 236
common, 236
date and time, recorded in log file, 94, 160, 190, 229
default settings
creating multiple configuration files, 298
DEFAULT.CFG
using a different configuration file, 298
defaults
scan targets, 84, 102, 111, 145, 152, 181, 233

scan task, as template for other scan tasks, 169

definitions

task, 166

virus, xiii

Delete

in **Task** menu, 167

descriptions, of VirusScan program components, 28 to 30

Desktop Management Interface alerts, sending, 91, 107, 115, 125, 157, 187, 227

detection

options

adding scan targets, 143, 150 to 152, 178 to 179

adding scan targets in ScreenScan, 231 to 232

choosing for VirusScan in Scheduler, 178

choosing in the E-Mail Scan program component, 219 to 222

choosing in VirusScan Advanced, 150 to 154

configuring for Download Scan module, 110 to 112

configuring for E-mail Scan module, 97 to 102

configuring for Internet Filter module, 119 to 122

configuring for System Scan module, 82 to 87

removing scan targets, 151, 180, 232

Detection page

for VirusScan in the Scheduler, 178 to 183

in Download Scan module, 110 to 112

in E-mail Scan module, 97 to 102

in Internet Filter module, 119 to 122

in System Scan module, 82 to 87

in the E-Mail Scan program component, 219 to 222

in VirusScan Advanced, 150 to 154

detections, false, understanding, 71 to 72

direct drive access

disabling with VirusScan, 300

directories

scanning, 303

Disable

in **Task** menu, 135, 168

VShield, 132 to 135

disguising virus infections, xvii

disks

choosing as scan targets, 143, 150 to 152, 178 to 179, 231 to 232

floppy

as medium for virus transmission, xv to xvi

locking or write-protecting, 58, 60

distribution

of update files, recommended methods for, 196 to 197

of upgrade files, recommended methods for, 206 to 207

distribution of VirusScan

electronically and on CD-ROM disc, 33

over networks, 44 to 49

DMI alerts, sending, 91, 107, 115, 125, 157, 187, 227

document files, as agents for virus transmission, xvii to xviii

Download Scan module

configuring, 110 to 118

default response options for, 64 to 65

set up

using configuration wizard, 79
using VShield Properties dialog box, 110 to 118

E

Edit menu
Copy, 167
Paste, 167
educational services, description of, 260
EICAR "virus," use of to test installation, 52
electronic services, contacting for technical support, 259
e-mail
addresses for reporting new viruses to Network Associates, xxiii
as agent for virus transmission, xviii
client software
choosing in configuration wizard, 79
choosing in E-Mail Scan Properties dialog box, 97 to 102
supported in VShield, 74
E-mail Scan module
configuring, 97 to 109
set up
using configuration wizard, 78
using VShield Properties dialog box, 97 to 109
E-Mail Scan program component, default responses when virus found, 68 to 70
Emergency Disk
creating
on uninfected computer, 54
without the creation wizard, 59 to 60
files to copy for, 59
use of BOOTSCAN.EXE on, 54
use of to reboot system, 54
Enable
in **Task** menu, 168
in VShield shortcut menu, 132
encrypted viruses, xvii
Enterprise SecureCast, 235, 250
completing registration for, 250
features of, 237
free services with, 237
InfoPaks from, distribution via ME!, 252
setting up, 251
subscriber benefits of, 250
support resources for, 254
system requirements for, 236
troubleshooting, 252
unsubscribing from, 253
use of in conjunction with AutoUpdate, 196
use of in conjunction with AutoUpgrade, 206
using, 252
Eudora and Eudora Pro
as e-mail clients supported in VShield, 74
Excel files, as agents for virus transmission, xviii
Exchange
as e-mail client supported in VShield, 74
exclusion options, choosing
for System Scan module, 95 to 97
for VirusScan Advanced, 161 to 163
for VirusScan in Scheduler, 191 to 193
executable programs
as agents for virus transmission, xvi
as tasks in VirusScan Scheduler, 171
Exit, in VShield shortcut menu, 132
expiration date message

disabling, 300
extended memory, setting VirusScan not to use, 300
extensions, use of to identify scan targets, 84, 102, 111, 145, 152, 181, 233

F

false detections, understanding, 71 to 72
File Info
in **File** menu, 71
file information, viewing, 70 to 71
File menu
File Info, 71
View Activity Log, 160, 190, 210
file name extensions
use of to identify vulnerable files, 84, 102, 111, 145, 152, 181, 233
File Transfer Protocol (FTP)
use of to obtain .DAT file updates, 196
use of to obtain VirusScan upgrades, 206
file validation using VALIDATE.EXE, 50 to 51
file-infecting viruses
definition and behavior of, xvi
setting heuristic scanning options for, 84 to 86, 153 to 154, 181 to 182, 221 to 222
files
choosing as scan targets, 143, 150 to 152, 178 to 179, 220 to 222, 231 to 232
compressed, scanning, 101, 112, 152, 180, 232
deleting infected files, 297
infected
cleaning, 88 to 90, 103 to 104, 113 to 114, 147, 155 to 156, 184 to 186, 223 to 224
cleaning yourself when VirusScan cannot, 54
deleting, 88 to 90, 103 to 104, 113 to 114, 147, 155 to 156, 184 to 186, 223 to 224
moving, 88 to 90, 103 to 104, 113 to 114, 147, 155 to 156, 184 to 186, 223 to 224
MAILSCAN.TXT, as E-Mail program component log, 227 to 228
SCREENSCAN ACTIVITY LOG.TXT, as ScreenScan log, 234
VSCLOG.TXT, as VirusScan log, 148 to 149, 159 to 160, 188 to 189
VSHLOG.TXT, as VShield log, 93 to 94
WEBEMAIL.TXT, as VShield log, 108 to 109
WEBFLTR.TXT, as VShield log, 125 to 127
WEBINET.TXT, as VirusScan log, 116 to 117
floppy disks
locking or write-protecting, 58, 60
role in spreading viruses, xv to xvi
folders
choosing as scan targets, 143, 150 to 152, 178 to 179, 231 to 232
Force Update, use of to replace corrupted .DAT files, 204
frequency
determining for VirusScan, 298
FTP (File Transfer Protocol)
use of to obtain .DAT file updates, 196
use of to obtain VirusScan upgrades, 206

H

Help

displaying in VirusSCan Command Line, 298
displaying in VirusScan Command Line, 296
opening from the Scheduler, 168
opening from VirusScan Classic and VirusScan Advanced, 143
Help Topics
in **Help** menu, 143, 168
heuristic scanning
definition of, 84 to 86, 153 to 154, 181 to 182, 221 to 222
to target program viruses only, 301
history of viruses, xiii to xix
Home SecureCast, 235, 237
completing registration for, 238
downloading automatically, 238
downloads, initiating with, 239
features of, 237
free services with, 237
registering evaluation software with, 246
setting up, 238
support resources for, 254
system requirements for, 236
unsubscribing from, 238
updating registered software with, 239
using, 238
hostile objects
distinction between viruses and, xix
Java classes and ActiveX controls as, xviii to xix, 27

I

infected files
cleaning yourself when VirusScan cannot, 54
deleting
recorded in log file, 94, 109, 117, 160, 190, 228
deleting permanently, 297
moving, 89, 103, 114, 147, 156, 185, 299
recorded in log file, 94, 109, 117, 160, 190, 228
removing viruses from, 53 to 70
use of quarantine folder to isolate, 89, 103, 114, 147, 156, 185, 224
installation
"silent," performing, 44 to 49
aborting if virus detected during, 53 to 55
testing effectiveness of, 52
Internet
dangers from, 27
e-mail clients, choosing
in configuration wizard, 78
in E-mail Scan Properties dialog box, 99
spread of viruses via, xviii
Internet Explorer
as browser supported in VShield, 74
Internet Filter module
configuring, 118 to 128
default response options for, 66
set up
using configuration wizard, 80
using VShield Properties dialog box, 118 to 128
Internet Relay Chat
as agent for virus transmission, xix
ISeamless
as a Network Associates scripting tool, 47

J

Java classes
- as malicious software, xviii to xix, 27
- distinction between viruses and, xix

L

last access dates, preserving on Novell NetWare drives, 301
local drives, scanning, 296
log file
- creating with text editor, 93 to 94, 108 to 109, 116 to 117, 125 to 127, 148 to 149, 159 to 160, 188 to 189, 227 to 228, 234
- information recorded in, 94, 109, 117, 160, 190, 228
- limiting size of, 94, 109, 117, 127, 149, 160, 189, 201, 210, 228
- MAILSCAN.TXT as, 227 to 228
- SCREENSCAN ACTIVITY LOG.TXT as, 234
- UPDATE UPGRADE ACTIVITY.TXT as, 200, 210
- VSCLOG.TXT as, 148 to 149, 159 to 160, 188 to 189
- VSHLOG.TXT as, 93 to 94
- WEBEMAIL.TXT as, 108 to 109
- WEBFLTR.TXT as, 125 to 127
- WEBINET.TXT as, 116 to 117

logging options. *See* report options
Lotus cc:Mail
- as e-mail client supported in VShield, 74
- choosing correct options for
  - in configuration wizard, 78
  - in E-mail Scan Properties dialog box, 99
  - logging on to and scanning v6.0 and v7.0 mailboxes, 229 to 230

LZEXE files, scanning, 83, 101, 112, 144, 152, 180, 220
LZH files, scanning, 101, 112, 144, 152, 180, 220, 232

M

macro viruses
- cleaning from Microsoft Office files, 297
- Concept virus, xvii to xviii
- definition and behavior of, xvii to xviii
- setting heuristic scanning options for, 84 to 86, 153 to 154, 181 to 182, 221 to 222

MAILSCAN.TXT, as E-Mail Scan program component report file, 227 to 228
malicious software
- ActiveX controls as, xviii to xix, 27
- distinction between hostile objects and viruses, xix
- Java classes as, xviii to xix, 27
- payload, xv
- script viruses as, xix
- spread via World Wide Web, xviii to xix
- types
  - Trojan horses, xv
  - worms, xiv

MAPI (Messaging Application Programming Interface) e-mail clients
- choosing in configuration wizard, 78
- choosing in E-mail Scan Properties dialog box, 99
- supported in VShield, 74

master boot record (MBR), susceptibility to virus infection, xvi
McAfee Emergency Disk

creating
on uninfected computer, 54
files to copy for, 59
use of to reboot system, 54
McAfee Enterprise (ME!), InfoPak distribution with, 252
memory
extended memory
setting VirusScan not to use, 300
omitting from scan operations, 300
preventing VShield from being removed from, 300
scanning as part of scan task, 183
to load VShield files into XMS memory, 304
unloading VShield from, 301
virus infections in, xv to xvi
menus, shortcut
use of from system tray
for VirusScan Scheduler, 166
for VShield, 132
use of in VirusScan Scheduler window, 166
messages
pausing when displaying, 301
Microsoft
Exchange, Outlook and Outlook Express, as e-mail clients supported in VShield, 74
Internet Explorer
as browser supported in VShield, 74
Visual Basic, as macro virus programming language, xviii
Word and Excel files, as agents for virus transmission, xviii
Microsoft Office
command to clean all macros from, 297
omitting files from scans, 300
military time, using to schedule scan tasks, 174
mIRC script virus, xix
mutating viruses, definition of, xvii

N

Netscape Navigator and Netscape Mail
as browser and e-mail client supported in VShield, 74
NetShield, use of
with the E-Mail Scan program component, 225
with VirusScan, 157, 187
with VShield, 91, 105, 115, 125
network alert, sending, 91, 105, 115, 125, 157, 187, 225
Network Associates
consulting services from, 259
contacting
Customer Care, xxi
outside the United States, xxiv
via America Online, xxi
via CompuServe, xxi
within the United States, xxii
educational services, 260
support services, 255
training, xxii, 259
website address for software updates and upgrades, 258
network deployment of VirusScan, 44 to 49
new scan task, creating, 167, 170 to 172
New Task
in **Task** menu, 167, 170
new viruses, reporting to Network Associates, xxiii

Novell NetWare drives, preserving last access dates on, 301
numbering conventions for .DAT files, 196

O

objects, Java and ActiveX
  as malicious software, xviii to xix, 27
Office, Microsoft
  command to clean all macros from, 297
  omitting files from scans, 300
Office, Microsoft, files as agents for virus transmission, xviii
online help
  opening from the Scheduler, 168
  opening from VirusScan Classic and VirusScan Advanced, 143
options
  Download Scan module, configuring, 110 to 118
  E-mail Scan module, configuring, 97 to 109
  E-Mail Scan program component
    Action, 222 to 224
    Alert, 225 to 227
    configuring, 218 to 229
    Detection, 219 to 222
    Report, 227 to 229
  Internet Filter module, configuring, 118 to 128
  ScreenScan, configuring, 230 to 234
  Security module, configuring, 128 to 132
  System Scan module, configuring, 82 to 97
  VirusScan
    Action, 183 to 186
    Alert, 186 to 188
    configuring, 176 to 195
    Detection, 178
    Exclusion, 191 to 193
    Report, 188 to 190
    Security, 193 to 195
  VirusScan Advanced
    Action, 154 to 156
    Alert, 156 to 160
    Detection, 150 to 154
    Exclusion, 161 to 163
    Report, 159 to 160
    Security, 163 to 164
  VirusScan Classic
    Action, 146 to 147
    Report, 148 to 149
    Where & What, 143 to 146
origin of viruses, xiii to xix
Outlook and Outlook Express
  as e-mail clients supported in VShield, 74
  distinguishing between, 79
overview, of VirusScan Scheduler, 167 to 168

P

panic, avoiding when your system is infected, 53
password, choosing
  for VirusScan in Scheduler, 194
  in VirusScan Advanced, 163
  in VShield Security module, 130
Paste
  in **Edit** menu, 167
pausing
  when displaying VirusScan messages, 301

payload, definition of, xv
PC viruses, origins of, xv
PKLite files, scanning, 83, 101, 112, 144, 152, 180, 220
plain text, use of to transmit viruses, xix
polymorphic viruses, definition of, xvii
POP-3 e-mail clients, choosing options for
  in configuration wizard, 79
  in E-mail Scan dialog box, 99
pranks, as virus payloads, xv
PrimeSupport
  Anytime, options, 256
  at a glance, 257
  availability, 258
  Basic, options, 255
  Extended, options, 256
  ordering, 258
Professional Consulting Services
  description of, 259
program components, included with VirusScan, 28 to 30
program extensions, designating as scan targets, 84, 102, 111, 145, 152, 181, 233
programs
  running after successful updates, 205
programs, running from VirusScan Scheduler, 171
Properties
  configuring for VirusScan, 176 to 195
  Download Scan module, configuring for, 110 to 118
  E-mail Scan module, configuring for, 97 to 109
  in **Task** menu, 167
  in VShield shortcut menu, 75, 82
  Internet Filter module, configuring for, 118 to 128
  Security module, configuring for, 128 to 132
  System Scan module, configuring for, 82 to 97
  VShield
    setting with configuration wizard, 75 to 81
property pages
  locking and unlocking, 131, 163, 194
proxy servers, working through to obtain updates and upgrades, 203, 213

Q

Qualcomm Eudora and Eudora Pro
  as e-mail clients supported in VShield, 74
quarantine folder, use of to isolate infected files, 89, 103, 114, 147, 156, 185, 224
quick start for VShield configuration, 75 to 81
quitting VShield, 132 to 135

R

RAM
  scanning as part of scan task, 183
  virus infections in, xv to xvi
reasons to run VShield, 73
rebooting, with the McAfee Emergency Disk, 54
Recycle Bin, excluded from scheduled scan operations, 95, 161, 192
registration
  for Enterprise SecureCast, 250
  for Home SecureCast, 238
remover

actions available when VirusScan has none, 54

report file

limiting size of, 94, 109, 117, 127, 149, 160, 189, 201, 210, 228

MAILSCAN.TXT as, 227 to 228

SCREENSCAN ACTIVITY LOG.TXT as, 234

UPDATE UPGRADE ACTIVITY.TXT as, 200, 210

VSCLOG.TXT as, 148 to 149, 159 to 160, 188 to 189

VSHLOG.TXT as, 93 to 94

WEBEMAIL.TXT as, 108 to 109

WEBFLTR.TXT as, 125 to 127

WEBINET.TXT as, 116 to 117

report options, choosing

for VirusScan in Scheduler, 188 to 190

in Download Scan module, 116 to 118

in E-mail Scan module, 108 to 109

in Internet Filter module, 125 to 128

in System Scan module, 93 to 95

in the E-Mail Scan program component, 227 to 229

in VirusScan Advanced, 159 to 160

in VirusScan Classic, 148 to 149

reporting viruses not detected to Network Associates, xxiii

reports

adding names of corrupted files to, 302

adding names of scanned files to, 302

adding system errors to, 303

centralized, settings for in .VSC file, 263

generating with VirusScan, 297, 302

rescue disk, creating without the creation wizard, 59 to 60

response options

choosing

when Download Scan module finds a virus, 64 to 65

when E-mail Scan module finds a virus, 62 to 64

when Internet Filter module finds harmful objects, 66

when System Scan module finds a virus, 60 to 62

when the E-Mail Scan program component detects a virus, 68 to 70

when VirusScan detects a virus, 66 to 68

setting

for Download Scan module, 112 to 114

for E-mail Scan module, 102 to 104

for Internet Filter module, 123

for System Scan module, 87 to 90

for VirusScan Advanced, 154 to 156

for VirusScan Classic, 146 to 147

for VirusScan in Scheduler, 183 to 186

responses, default, when infected by viruses, 53 to 70

restarting

with CTRL+ALT+DEL, ineffective use of to clear viruses, xvi

with the McAfee Emergency Disk, 54

results

displayed in VShield Status dialog box, 136 to 137

scan task status, 175

retail customers, support features included with purchase, 258

right-clicking

use of to display shortcut menus for VShield, 132

use of to display shortcut menus in VirusScan Scheduler, 166
rollout, of VirusScan over networks, 44 to 49

S

scan operations, deciding when to start, 31
scan task
action options, configuring, 146 to 147, 154 to 156, 183 to 186
alert options, configuring, 156 to 160, 186 to 188
boot blocks, examining as part of, 183
configuring
options for in VirusScan Scheduler, 176 to 195
copying settings from one to another, 167
Default Scan as template for, 169
defaults
included with VirusScan Scheduler, 169
definition of, 166
deleting, 167
detection options
choosing for VirusScan in Scheduler, 178
configuring in VirusScan Advanced, 150 to 154
disabling, 168
entering schedule times for, 174
excluding items from, 191 to 193
exclusion options, configuring
for VirusScan Advanced, 161 to 163
for VirusScan in Scheduler, 191 to 193
logging options, configuring
for VirusScan in Scheduler, 188 to 190
in VirusScan Advanced, 159 to 160
in VirusScan Classic, 148 to 149
memory, scanning, 183
naming, 171
new, creating, 167, 170 to 172
pasting settings from another, 167
program to carry out, choosing, 171
removing, 167
report options, configuring
for VirusScan Advanced, 159 to 160
for VirusScan Classic, 148 to 149
for VirusScan in Scheduler, 188 to 190
schedule times and intervals available for, 173
scheduling and enabling, 167, 172 to 174
security options, configuring, 163 to 164, 193 to 195
speeding up, 161 to 163
starting, 168
automatically, 183
need for Scheduler to be running, 174
status, checking, 175
stopping, 168
targets for
adding, 143, 150 to 152, 178 to 179, 231 to 232
removing, 151, 180, 232
Where & What options, configuring, 143 to 146
scan tasks
scheduling and enabling
as purpose of Scheduler, 165
possible applications for, 165
speeding up, 191 to 193
scanning
excluding items from, 161 to 163
speeding up scan times, 161 to 163

Scheduler
action options for VirusScan, configuring from, 183 to 186
alert options for VirusScan, configuring from, 186 to 188
commands available in, 167 to 168
configuring tasks in, 167, 176 to 195
copying and pasting tasks in, 167
creating new tasks in, 167, 170, 172
default scan tasks included with, 169
definition of scan task in, 166
deleting tasks from, 167
detection options for VirusScan, configuring from, 178 to 183
disabling and enabling tasks from, 168
exclusion options for VirusScan, configuring from, 191 to 193
icon in system tray, 166
in **Tools** menu, 166
necessity to have running to start scan tasks, 174
overview of, 167 to 168
possible applications for, 165
purpose of, 165
report options for VirusScan, configuring from, 188 to 190
scheduling and enabling tasks in, 167, 172 to 174
security options for VirusScan, configuring from, 193 to 195
starting, 166
starting tasks from, 168
status bar in, hiding and displaying, 167
stopping tasks from, 168
title bar in, hiding and displaying, 167
toolbar in, hiding and displaying, 166
use of to run executable programs, 171
VShield as scan task in, 169
window, elements of, 166
SCREENSCAN ACTIVITY LOG.TXT, as ScreenScan report file, 234
script viruses, xix
SecureCast
additional files delivered by, 236
common data files delivered by, 236
downloads, initiating with, 239
Enterprise SecureCast, 235, 250
completing registration for, 250
InfoPaks from, distribution via ME!, 252
setting up, 251
subscriber benefits of, 250
troubleshooting, 252
unsubscribing from, 253
using, 252
features of, 237
free services with, 237
Home SecureCast, 235, 237
completing registration for, 238
downloading automatically, 238
registering evaluation software with, 246
setting up, 238
unsubscribing from, 238
updating registered software with, 239
using, 238
support resources for, 254
system requirements for, 236
updating your software with, 235
security
password, choosing, 131, 163, 194
Security module

configuring, 128 to 132
security options
choosing for VirusScan Advanced, 163 to 164
choosing for VirusScan in Scheduler, 193 to 195
Select, 167
session settings
recorded in log file, 94, 109, 118, 160, 190, 229
session summary
recorded in log file, 94, 109, 118, 160, 190, 229
settings
VShield, choosing with configuration wizard, 75 to 81
Setup
"silent" and "record" modes, using, 44, 49
aborting if virus detected during, 53 to 55
SETUP.ISS file, use of, 45 to 49
shortcut menus
use of in VirusScan Scheduler window, 166
use of with VShield, 132
signatures, use of for virus detection, xvii
"silent" installation, performing, 44 to 49
SMTP e-mail clients
choosing options for
in configuration wizard, 79
in E-mail Scan Properties dialog box, 99
software conflicts, as potential cause for computer problems, 31 to 32
software updates and upgrades, website address for obtaining, 258
spreadsheet files, virus infections in, xvii to xviii
Start
in **Task** menu, 168
Start menu
using to start VirusScan Classic, 140, 149
statistics
displayed in VShield Status dialog box, 136 to 137
for scan task, 175
status
checking for scan operations, 175
checking for VShield, 136 to 137
Status Bar
in **View** menu, 167
in VirusScan Scheduler, hiding and displaying, 167
Status dialog box
using to disable and enable VShield modules, 133
stealth viruses, definition of, xvii
Stop
in **Task** menu, 168
VShield, 132 to 135
subdirectories
scanning, 303
support
for retail customers, options, 258
hours of availability, 259
PrimeSupport
Anytime, 256
at a glance, 257
availability, 258
Basic, 255
Extended, 256
ordering, 258

resources for SecureCast, 254
via electronic services, 259
system crashes, attributing to viruses, 53
system files, as agents for virus transmission, xvi
system requirements
for SecureCast, 236
for VirusScan, 33
System Scan
in VShield shortcut menu, 75, 82
System Scan module
configuring, 82 to 97
default response options for, 60 to 62
set up
using configuration wizard, 77
using VShield Properties dialog box, 82 to 97
system tray
location of VirusScan Scheduler icon, 166
location of VShield icon, 75, 82

T

targets for scanning
adding, 143, 150 to 152, 178 to 179, 231 to 232
removing, 151, 180, 232
task
action options, configuring, 146 to 147, 154 to 156, 183 to 186
adding scan targets to, 143, 150 to 152
alert options, configuring, 156 to 160, 186 to 188
configuring options for in VirusScan Scheduler, 176 to 195
copying settings from one to another, 167
Default Scan as template for, 169
defaults, included with VirusScan Scheduler, 169
definition of, 166
deleting, 167
detection options
choosing for VirusScan in Scheduler, 178 to 183
configuring in VirusScan Advanced, 150 to 154
disabling and enabling, 168
entering schedule times for, 174
exclusion options, configuring
for VirusScan Advanced, 161 to 163
for VirusScan in Scheduler, 191 to 193
logging options, configuring
for VirusScan in Scheduler, 188 to 190
in VirusScan Advanced, 159 to 160
in VirusScan Classic, 148 to 149
memory, scanning as part of, 183
naming, 171
new, creating, 167, 170 to 172
pasting settings from another, 167
program to carry out, choosing, 171
removing, 167
removing scan targets, 151, 232
report options, configuring
for VirusScan Advanced, 159 to 160
for VirusScan Classic, 148 to 149
for VirusScan in Scheduler, 188 to 190
running executable programs as part of, 171
scan targets for
adding, 178 to 179, 231 to 232
removing, 180

schedule times and intervals available for, 173
scheduling and enabling, 167, 172 to 174
security options, configuring, 163 to 164, 193 to 195
starting, 168
automatically, 183
need for Scheduler to be running, 174
status, checking, 175
stopping, 168
Where & What options, configuring, 143 to 146
task list
default tasks in, 166
Task menu
Delete, 167
Disable, 135, 168
Enable, 168
New Task, 167, 170
Properties, 167
Start, 168
Stop, 168
View Activity Log, 201
taskbar
location of VirusScan Scheduler icon in, 166
location of VShield icon in, 75, 82
.TD0 files, scanning, 101, 112, 144, 152, 180, 220
technical support
e-mail address for, xxi
features included with retail purchase, 258
hours of availability, 259
information needed from user, xxii
online, xxi
phone numbers for, xxii
PrimeSupport
Anytime, 256
at a glance, 257
availability, 258
Basic, 255
Extended, 256
ordering, 258
via electronic services, 259
template, for scan tasks, 169
testing your installation, 52
text
editor, use of to create log file, 93 to 94, 108 to 109, 116 to 117, 125 to 127, 148 to 149, 159 to 160, 188 to 189, 227 to 228, 234
messages, use of to transmit viruses, xix
Title Bar
in **View** menu, 167
in VirusScan Scheduler, hiding and displaying, 167
Toolbar
in **View** menu, 167
in VirusScan Scheduler, hiding and displaying, 166
Tools menu
Scheduler, 166
Total Education Services
description of, 259
Total Service Solutions
contacting, 259
Total Virus Defense
VirusScan as component of, 27
training for Network Associates products, xxii, 259
scheduling, xxii

Trojan horse, definition of, xv
troubleshooting
firewall problems, 252
registration problems, 252
24-hour clock, using to enter schedule times, 174

U

uninfected computer, use of to create Emergency Disk, 54
Universal Naming Convention (UNC) notation, use of to designate update and upgrade sites, 202, 212
unsubscribing
from Home SecureCast, 238
UPDATE UPGRADE ACTIVITY.TXT
as AutoUpdate and AutoUpgrade log file, 200, 210
UPDATE.INI, as settings file for AutoUpdate, 201, 203, 205
updates
automatic, via AutoUpdate, 196 to 205
recommended method for downloading and distributing, 196 to 197
updates and upgrades
distinction between, 196, 206
use of anonymous FTP to log into sites for, 202, 212
use of UNC notation to designate, 202, 212
updates and upgrades, website address for obtaining, 258
UPGRADE.INI, as settings file for AutoUpgrade, 211, 213 to 214
upgrades
automatic, via AutoUpgrade, 206 to 214
recommended method for downloading and distributing, 206 to 207
user name, recorded in log file, 94, 160, 190, 229

V

VALIDATE.EXE, use of to verify Network Associates software, xx, 50 to 51
View Activity Log
in **File** menu, 160, 190
in **Task** menu, 190, 201, 210
View menu
Status Bar, 167
Title Bar, 167
Toolbar, 167
Virus List, 168
Virus Information Libarary, connecting to from VirusScan, 70 to 71
Virus Information Library
use of to learn how to remove viruses, 55
Virus List
in **View** menu, 168
viruses
"Brain" virus, xv
boot-sector infectors, xv to xvi
cleaning, recorded in log file, 94, 160, 190, 228
code signatures, use of by, xvii
Concept, xvii to xviii
costs of, xiii to xiv
current numbers of, xiii
deciding when to start scan operations for, 31
default response to
when E-Mail Scan program component detects, 68 to 70
when VirusScan detects, 66 to 68
when VShield detects, 60 to 66

definition of, xiii
detecting, recorded in log file, 94, 109, 117, 160, 190, 228
disguising infections of, xvii
displaying list of those detected in VirusScan Command Line, 304
distinction between hostile objects and, xix
effects of, xiii, 53 to 70
encrypted, definition of, xvii
false detections of, understanding, 71 to 72
file infectors, xvi
history of, xiii to xix
macro, xvii to xviii
setting heuristic scanning options for, 84 to 86, 153 to 154, 181 to 182, 221 to 222
mutating, definition of, xvii
origins of, xiii to xix
payload, xv
polymorphic, definition of, xvii
programs similar to
Trojan horses, xv
worms, xiv
recognizing when computer problems do not result from, 31 to 32
removing
before installation, necessity of and steps for, 53 to 55
from infected files, 53 to 70
reporting new strains to Network Associates, xxiii
role of PCs in spread of, xv
script language, xix
spread of via e-mail and Internet, xviii
stealth, definition of, xvii
viewing information about, 70 to 71
why worry?, xiii to xiv
VirusScan
Action options
choosing for in Scheduler, 183 to 186
configuring in VirusScan Advanced, 154 to 156
configuring in VirusScan Classic, 146 to 147
alert messages
sending via DMI, 157, 187
Alert options
choosing in Scheduler, 186 to 188
configuring in Advanced mode, 156 to 158
as component of Total Virus Defense suite, 27
BIOS anti-virus features, potential conflicts with, 72
command-line examples, 296
components included with, 28 to 30
configuring for scan operations, 176 to 195
default responses to virus detection, 66 to 68
description of program components, 28 to 30
detection options
choosing in Scheduler, 178
configuring in VirusScan Advanced, 150 to 154
distribution methods, 33
exclusion options
choosing in Scheduler, 191 to 193
configuring in VirusScan Advanced, 161 to 163
files to copy for Emergency Disk, 59

generating a report file, 297, 302 to 303
installation
"silent", 44 to 49
as best protection against infection, 53
what to do when virus found during, 53 to 55
introducing, 27
logging options, choosing in Scheduler, 188 to 190
main window
use of to select responses to infections, 67
overview of features, 27
password protection, configuring, 163
preventing users from halting, 299
property pages
Action, 146 to 147, 154 to 156, 183 to 186
Alert, 156 to 160, 186 to 188
Detection, 150 to 154, 178 to 183
Exclusion, 161 to 163, 191 to 193
Report, 159 to 160, 188 to 190
Security, 193 to 195
Where & What, 143 to 146
report options
choosing in Scheduler, 188 to 190
configuring in VirusScan Advanced, 159 to 160
security options, choosing in Scheduler, 193 to 195
setting the scan frequency, 298
updating via AutoUpdate, 196 to 205
upgrading via AutoUpgrade, 206 to 214
validating with VALIDATE.EXE, 50
ways to use, 139
what it does, 139
VirusScan Advanced
Action options, choosing, 154 to 156
Alert options, choosing, 156 to 160
Detection options, choosing, 150 to 154
Exclusion options, choosing, 161 to 163
password protection, configuring, 163
property pages
Heuristics, 153, 181, 221
Report options, choosing, 159 to 160
Security options, choosing, 163 to 164
using the start the Scheduler, 166
VirusScan Classic
Action options, choosing, 146 to 147
Report options, choosing, 148 to 149
starting, 140, 149
Where & What options, choosing, 143 to 146
VirusScan Command Line
use of when booting with Emergency Disk, 54
VirusScan command-line options
/? or /HELP, 296, 298
/ADL, 296
/ADN, 296
/ALERTPATH, 296
/ALL, 296
/ANALYZE, 296
/ANYACCESS, 297
/APPEND, 297
/BOOT, 297
/BOOTACCESS, 297
/CLEAN, 297
/CLEANDOCALL, 297
/CONTACT, 297

/CONTACTFILE, 297
/DEL, 297
/EXCLUDE, 298
/FILEACCESS, 298
/FREQUENCY, 298
/HELP, 296, 298
/IGNORE, 298
/LOAD, 298
/LOCK, 298
/MANALYZE, 298
/MANY, 299
/MAXFILESIZE, 299
/MEMEXCL, 299
/MOVE, 299
/NOBEEP, 299
/NOBREAK, 299
/NOCOMP, 299
/NODDA, 300
/NODISK, 300
/NODOC, 300
/NOEMS, 300
/NOEXPIRE, 300
/NOMEM, 300
/NOREMOVE, 300
/NOWARMBOOT, 300
/NOXMS, 300
/ONLY, 300
/PANALYZE, 301
/PAUSE, 301
/PLAD, 301
/RECONNECT, 301
/REMOVE, 301
/REPORT, 302
/RPTALL, 302
/RPTCOR, 302
/RPTERR, 303
/SAVE, 303
/SUB, 303
/UNZIP, 303
/VIRLIST, 304
/XMSDATA, 304
VirusScan Scheduler, 167 to 168
action options for VirusScan, configuring from, 183 to 186
alert options for VirusScan, configuring from, 186 to 188
configuring tasks in, 167, 176 to 195
copying and pasting tasks in, 167
creating new tasks in, 167, 170, 172
default scan tasks included with, 169
deleting tasks from, 167
detection options for VirusScan, configuring from, 178 to 183
disabling and enabling tasks from, 168
disabling and enabling VShield from, 134
icon in system tray, 166
necessity to have running to start scan tasks, 174
overview of, 167 to 168
possible applications for, 165
purpose of, 165
scheduling and enabling tasks in, 167, 172 to 174
starting, 166
starting tasks from, 168
status bar in, hiding and displaying, 167
stopping tasks from, 168
title bar in, hiding and displaying, 167
toolbar in, hiding and displaying, 166
use of to run executable programs, 171

VShield as scan task in, 169

window, elements of, 166

Visual Basic, as macro virus programming language, xviii

VSCLOG.TXT, as VirusScan report file, 148 to 149, 159 to 160, 188 to 189

VShield

alert messages

sending via DMI, 91, 107, 115, 125

as scan task in VirusScan Scheduler window, 169

browsers and e-mail clients supported in, 74

configuration wizard

starting, 75

using, 75 to 81

default responses to virus detection, 60 to 66

disabling and enabling, 132 to 135

Download Scan module

configuring, 110 to 118

default response options for, 64 to 65

E-mail Scan module

configuring, 97 to 109

default response options for, 62 to 64

icon in system tray, 75, 82

using to disable VShield, 132

Internet Filter module

configuring, 118 to 128

default response options for, 66

Properties dialog box

Download Scan module, 110, 118

E-mail Scan module, 97, 109

Internet Filter module, 118, 128

Security module, 128, 131

System Scan module, 82 to 87

using to disable and enable VShield modules, 133 to 134

Wizard button in, 76

reasons to run, 73

Security module

configuring, 128 to 132

shortcut menu

Enable, 132

Exit, 132

Properties, 75, 82

System Scan, 75, 82

single task only available in Scheduler, 176

Status dialog box, using to disable and enable VShield modules, 133

stopping and unloading from memory, 132 to 135

System Scan module

configuring, 82 to 97

default response options for, 60 to 62

unloading from memory, 132 to 135

what it does, 73

Vshield

components included with VirusScan, 28 to 30

VSHLOG.TXT, as VShield report file, 93 to 94

W

warm boot, ineffective use of to clear viruses, xvi

WEBEMAIL.TXT, as VShield logging file, 108 to 109

WEBFLTR.TXT, as VShield logging file, 125 to 127

WEBINET.TXT, as VirusScan logging file, 116 to 117

website, Network Associates technical support via, 259

Where & What options

choosing in VirusScan Classic, 143 to 146

why worry about viruses?, xiii to xiv

window elements, in VirusScan Scheduler, 166

Windows Compressed files (.??_), scanning, 101, 112, 144, 152, 180, 220

Windows Start menu, using to start VirusScan Classic., 140, 149

Wizard, button in VShield Properties dialog box, 76

Word files, as agents for virus transmission, xviii

World Wide Web, as source of malicious software, xviii to xix

worms, definition of, xiv

write protection, enabling for floppy disks, 58, 60

Z

.ZIP files, scanning, 101, 112, 144, 152, 180, 220, 232